Barracuda SSL VPN Administrator's Guide

Version 1.0

Barracuda Networks Inc.
3175 S. Winchester Blvd
Campbell, CA 95008
http://www.barracuda.com

Copyright Notice

Copyright 2008, Barracuda Networks
www.barracudanetworks.com
v1x-081201-01-1201

All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.

Trademarks

Barracuda SSL VPN is a trademark of Barracuda Networks. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders.

INTRODUCTION **6**

GETTING STARTED **9**

Deployment Scenarios 15
Configuring your Firewall to Route Incoming SSL Connections to the Barracuda SSL VPN 16
Testing Connections to the Barracuda SSL VPN 16

APPLIANCE ADMINISTRATOR WEB INTERFACE **18**

Monitoring the Barracuda SSL VPN 19
Viewing the Status Page Graphs 19
Configuring the Appliance Administrator Interface Ports 19
Configuring Network Information 19

SSL VPN ADMINISTRATOR WEB INTERFACE **23**

Purpose 23
Switching Views 23
Accessibility 24
Monitoring the Barracuda SSL VPN 24
Viewing the Status Page Graphs 24

CONFIGURING USER DATABASES **25**

Configure User Database 25
Configuring the Built-in Database 25
Configuring Active Directory 25
Configuring Enhanced Active Directory 27
Configuring LDAP 30
Configuring NIS User Database 31

ADVANCED SYSTEM CONFIGURATION **32**

User Interface 32
Password Options 33
Session Options 33
Confidential Attributes 34

APPEARANCE **35**

Logon Page 35

SSL CERTIFICATES **36**

SSL Certificates Interface 36
Creating a CA 37
Importing a Certificate 38
Exporting Keys and Certificates 40

ATTRIBUTES **41**

Attribute Interface 43
Creating Attributes 44
Editing an Attribute 45
Deleting an Attribute 45
How to use Attributes 46

ACCESS CONTROL **48**

Overview 48
Access Control Architecture 49

CREATING ACCOUNTS 52

Principal Types 52
Administrator Account 52
Account Interface 52
Create New Account 53
Editing an Account 54
Deleting an Account 54

CREATING GROUPS 55

What are Groups? 55
Groups Interface 56
Create New Group 56
Editing a Group 56
Delete Group 56

CREATING POLICIES 57

What is a Policy? 57
Policy Interface 58
Create Policy 58
Editing a Policy 60
Delete Policy 60

CREATING ACCESS RIGHTS 61

What is a Resource? 61
What are Access Rights? 61
Access Rights Interface 61
Creating an Access Right 62
Editing Access Rights 63
Delete Access Rights 63

AUTHENTICATION SCHEMES 64

What is an Authentication Scheme? 64
Creating an Authentication Scheme 65
Deleting an Authentication Scheme 66
Authentication Modules 67
Password Authentication 67
Personal Questions Authentication 70

***RESOURCE MANAGEMENT* 72**

What are Resources? 72
Resource Wizards 72
Available Resources 72
Executing a Resource 73

THE BARRACUDA SSL VPN AGENT 74

What is the Barracuda SSL VPN Agent? 74
Executing Resources from the Barracuda SSL VPN Agent 75

***WEB FORWARDING* 76**

What is a Web Forward? 76
Web Forward Interface 78

Creating a new Web Forward 79
Editing a Web Forward 85
Deleting a Web Forward 85
Outlook Web Access and Mail Check 86

NETWORK PLACES **88**

What is a Network Place? 88
Network Places Interface 89
Creating a new Network Place 90
Editing a Network Place 94
Deleting a Network Place 94
Web Folders Windows Access 94
Windows Explorer Drive Mapping 99

APPLICATIONS **101**

What is an Application Shortcut? 101
Applications Interface 101
Publish a new Application 102
Edit an Existing Application 104
Removing an Application 104

SSL TUNNELS **105**

What is an SSL Tunnel? 105
SSL Tunnels Interface 105
Create a new SSL Tunnel 105
Edit an existing SSL Tunnel 108
Removing an SSL Tunnel 108

PROFILES **110**

What is a Profile? 110
Profiles Interface 110
Creating a new Profile 111
Editing Profile Parameters 112
Editing a Profile Description 114
Deleting a Profile 114

SYSTEM FUNCTIONS **116**

AUDITING **116**

Auditing Interface 116
Creating a New Report 117
Running One-Off Reports 119

LIMITED WARRANTY AND LICENSE **124**

Limited Warranty 124

Chapter 1
Introduction

This chapter provides an overview of the Barracuda SSL VPN and includes the following topics:

- Overview
- Barracuda SSL VPN Models

Overview

The Barracuda SSL VPN is an integrated hardware and software solution enabling secure, clientless remote access to internal network resources from any Web browser.

Designed for remote employees and road warriors, the Barracuda SSL VPN provides comprehensive control over file systems and Web-based applications requiring external access. The Barracuda SSL VPN integrates with third-party authentication mechanisms to control user access levels and provide single sign-on.

- Enables access to corporate intranets, file systems or other Web-based applications
- Tracks resource access through auditing and reporting facilities
- Scans uploaded files for viruses and malware
- Leverages multi-factor, layered authentication mechanisms, including RSA SecurID tokens
- Integrates with existing Active Directory and LDAP directories
- Utilizes policies for granular access control framework
- Supports any Web browser on PC or Mac

Energize Updates Minimize Administration and Maximize Protection

To provide you with maximum protection against the latest types of spam and virus attacks, Barracuda Networks maintains a powerful operations center called Barracuda Central. From this center, engineers monitor the Internet for trends in virus attacks and post updated definitions to Barracuda Central. These updates are then automatically retrieved on a regular basis by your Barracuda SSL VPN using the Energize Updates feature.

Energize Updates provide your Barracuda SSL VPN with the following benefits:

- Virus definitions constantly updated
- Maintenance and support from Barracuda Central
- Access to latest product updates

Technical Support

To contact Barracuda Networks Technical Support:

- By phone: call 1-408-342-5400, or if you are in the United States, (888) ANTI-SPAM, or (888) 268-4772
- By email: use *support@barracuda.com*
- Online: visit *http://www.barracuda.com/support* and click on the Support Case Creation link.

There is also a Barracuda Networks Support Forum available where users can post and answer other users' questions. Register and log in at *http://forum.barracuda.com*.

Warranty Policy

The Barracuda SSL VPN has a one (1) year warranty against manufacturing defects.

Barracuda SSL VPN Models

The Barracuda SSL VPN comes in a variety of models. Refer to the following table for the capacity and features available on each model:

Feature	*Model 280*	*Model 380*	*Model 480*
CAPACITY			
Recommended Max Users	25	50	100
HARDWARE			
Rackmount Chassis	1U Mini	1U Mini	1U Mini
Dimensions (in.)	16.8x1.7x14	16.8x1.7x14	16.8x1.7x14
Dimensions (cm.)	42.7x4.3x35.6	42.7x4.3x35.6	42.7x4.3x35.6
Weight (lbs. /kg.)	12 / 5.4	12 / 5.4	12 / 5.4
Ethernet	1 x 10/100	1 x 10/100	1 x 10/100
AC Input Current (Amps)	1.0	1.2	1.4
Redundant Disk Array (RAID)			✓
FEATURES			
SSL Tunneling	✓	✓	✓
Barracuda Network Connector	✓	✓	✓
Intranet Web Forwarding	✓	✓	✓
Network File Access	✓	✓	✓
Windows Explorer Mapped Drives	✓	✓	✓
VNC/NX/Telnet/SSH/RDP Applications	✓	✓	✓
Remote Desktop Single Sign-On	✓	✓	✓
Antivirus	✓	✓	✓
Virtual Keyboard	✓	✓	✓
Active Directory/LDAP Integration	✓	✓	✓
Layered Authentication Schemes	✓	✓	✓
Multiple User Realms		✓	✓
Barracuda SSL VPN Server Agent		✓	✓
Hardware Token Support			✓
RADIUS Authentication			✓
SNMP / API			✓
Syslog Logging			✓

Chapter 2
Getting Started

This chapter provides an overview of The Barracuda SSL VPN detailing the initial installation and the basics of interacting with the system through the Management Console.

- Initial Setup
- Installation Examples
- Firewall Configuration
- External Proxy Configuration

Initial Setup

Checklist for Unpacking

Thank you for purchasing the Barracuda SSL VPN. Match the items on this list with the items in the box. If any item is missing or damaged, please contact your Barracuda Networks Sales representative.

- Barracuda SSL VPN
- AC Power Cord
- Ethernet Cables

Required Equipment for Installation

These are items that are needed for installing the Barracuda SSL VPN:

- VGA monitor
- PS2 keyboard

Install the Barracuda SSL VPN

To physically install the Barracuda SSL VPN:

1. Fasten the Barracuda SSL VPN to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet Cable from your network switch to the Ethernet port on the back of the Barracuda SSL VPN.
3. Connect a Standard VGA Monitor, PS2 Keyboard, and AC power cord to the Barracuda. Note: Immediately after connecting an AC Power Cord to the Barracuda, it may power ON for a few seconds and then power OFF. This is because the Barracuda is designed to automatically return to a powered ON state in the event of a power outage.
4. Press the POWER button on the front panel to turn the appliance on.

APC UPS Support

An APC (American Power Conversion) UPS (Uninterruptible Power Supply) device with a USB interface is supported with the Barracuda SSL VPN. No configuration changes are needed on the Barracuda SSL VPN to use one.

When the APC UPS device is on battery power, the Web-based administration interface will display an alert and the Barracuda SSL VPN will shut down safely when there is an estimated 3 minutes of battery power remaining.

Configure the System IP Address and Network Settings

If you have a monitor connected, the Barracuda SSL VPN will display the Boot Menu initially and the Administrative Console login prompt once fully booted. To begin the configuration:

1. Login to the Administrative Console using the admin login:

   Login: admin

Password: admin

2. Configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server** and **Secondary DNS Server** as appropriate for your network.
3. Save your changes.

If you do not have a monitor and keyboard and want to set the IP using the RESET button on the front panel, press and hold the RESET button per the following table:

IP address	Press and hold RESET for…
192.168.200.200	5 seconds
192.168.1.200	8 seconds
10.1.1.200	12 seconds

Opening Firewall Ports

If your Barracuda SSL VPN is located behind a corporate firewall, ensure that the following ports on your firewall are open to ensure proper operation.

Port	Dir.	TCP	UDP	Usage
25	Out	Yes	No	Email alerts + One-time passwords
53	Out	Yes	Yes	Domain Name Service (DNS)
80	Out	Yes	No	Virus, firmware and updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	In/Out	Yes	No	HTTPS/SSL port for SSL VPN access
8000	In/Out	Yes	No	Appliance administrator interface port (HTTP)
8443	In/Out	Yes	No	Appliance administrator interface port (HTTPS)

Note: The Appliance Administrator interface ports on 8000/8443 should only be opened if you intend to manage the appliance from the Internet.

Configure the Barracuda SSL VPN

After specifying the IP address of the system and opening the necessary ports on your firewall, you will need to configure the Barracuda SSL VPN from the administration interface. Make sure the computer from which you configure the Barracuda SSL VPN is connected to the same network, and the appropriate routing is in place to allow connection to the Barracuda SSL VPN's IP address from a Web browser.

To configure the Barracuda SSL VPN:

1. In your Web browser's address bar, enter **http://** followed by the Barracuda SSL VPN's IP address, followed by the default Appliance Administrator Web interface HTTP port (:8000). For example, if you configured the appliance with an IP address of 192.168.200.200, you would type: http://192.168.200.200:8000
2. Log in to the administration interface by entering `ssladmin` for the username and `ssladmin` for the password.
3. Go to the **Basic→ IP Configuration** page and perform the following:
   - Verify that the **IP Address**, **Subnet Mask**, and **Default Gateway** are correct.
   - Verify that the **Primary** and **Secondary DNS Server** are correct.
   - Verify that the **Proxy Server Configuration** settings are correct, if you are using a proxy server on your network.
4. Click **Save Changes**. If you changed the IP address of your Barracuda SSL VPN, you are disconnected from the administration interface and will need to log in again using the new IP address.

Set the Administrative Options

To set the Administrative Options:

1. Select **Basic** → **Administration**.
2. Assign a new administration password to the Barracuda SSL VPN. You cannot change the password for the Administrative Console, but this is only accessible via the keyboard which you can disconnect at any time.
3. Set the local time zone. The time on the Barracuda SSL VPN is automatically updated via NTP (Network Time Protocol), which requires port 123 to be opened for outbound UDP traffic on the firewall.
4. Click **Save Changes**.

Update the System Firmware

Prior to upgrading the firmware on your Barracuda SSL VPN, it is always recommended that you read the release notes.

To upgrade the firmware on the Barracuda SSL VPN:

1. Select **Advanced** > **Firmware Update**.
2. Click **Download Now** and then **OK** on the download duration window.
Updating the firmware may take several minutes. Do not turn off the unit during this process. If the system has the latest firmware version downloaded, the **Download Now** button is disabled.
3. To see the download progress, click the **Refresh** button that appears next to the completion percentage. Once the download has finished, that button will turn into an **Apply Now** button.
4. Click **Apply Now** to activate the newly-downloaded firmware. This process will automatically reboot your system when completed, which can cause your Web interface to disconnect momentarily. **This is normal and expected behavior**, so there is no need to perform a manual reboot. The Web interface should come back up again within 5 minutes, at which point you will need to log in again.
5. Log back into the Appliance Administrator Web interface again and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings you may have already entered, as new features may have been included with the firmware update.

Product Activation

Verify that the Energize Updates feature is activated on your Barracuda by going to the **Basic > Status** page.

1. Under Subscription Status, make sure the Energize Updates subscription is Current. If the Energize Updates is Not Activated, click the corresponding activation link to go to the Barracuda Networks Product Activation page and complete activation of your subscriptions.
2. Reboot your Barracuda SSL VPN.

Route Incoming Connections to the Barracuda SSL VPN

To take advantage of the features of the Barracuda SSL VPN, you must route HTTPS incoming connections on port 443 to the Barracuda. This is typically achieved by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN:

Note: The Appliance Administrator Web interface ports on 8000/8443 will also need similar port forward configurations if you intend to manage the appliance from outside the corporate network.

Test the Connection to the Barracuda SSL VPN

Once you have configured your corporate firewall to route SSL through to the Barracuda SSL VPN, you should be able to accept incoming SSL connections.

1. To test the connection, use a Web browser from the Internet (not inside the LAN) to establish an SSL connection to the external IP address of your corporate firewall. For example, if your firewall's external IP address is 192.168.1.1, connect your browser: https://192.168.1.1
2. You should be prompted to accept an un-trusted SSL certificate, which will cause a warning message to appear in your browser. Accept the warning and proceed to load the page.
3. You should be prompted with the login page for the SSL VPN User Interface. Log in with the credentials for the VPN administrator:
    - Login: ssladmin
    - Password: ssladmin
4. You should have successfully logged in using the VPN administrator account and will be taken directly to the SSL VPN Management Interface. From here you can now proceed to set up accounts and other resources for users of the Barracuda SSL VPN.

Post Setup Configuration Items

Your Barracuda SSL VPN should now be configured at a basic level to accept incoming connections from the Internet. You should next consult your product documentation to:

- Register a hostname with your DNS server for the Barracuda SSL VPN e.g. *sslvpn.company.dom*
- Install an SSL certificate on the Barracuda SSL VPN for this hostname to ensure your users are able to determine that they are connecting to a genuine Barracuda SSL VPN that is registered to your organization.
- Integrate the Barracuda SSL VPN with your existing user database. To cleanly integrate with your environment, the Barracuda can read in user accounts and authenticate against a number of different databases, including Microsoft Active Directory.
- Grant access to resources to your SSL VPN users. See the documentation for more information on the usage of the policy based access control framework.
- If your network uses a DMZ you may wish to configure the Barracuda SSL VPN in this topology for greater security.

Verify your Subscription Status

When you install the Barracuda SSL VPN, your Energize Updates and Instant Replacement subscriptions are active. It is important you verify the subscription status so your Barracuda SSL VPN receives the latest virus definitions and updates from Barracuda Central. The Energize Update service is responsible for downloading these virus and spam definitions to your system.

Note

ALWAYS read the release notes prior to downloading a new firmware version. Release notes provide you with information on the latest features and fixes provided in the updated firmware version. You can access the release notes from the **Advanced** > **Firmware Update** page.

Note
The apply process takes several minutes to complete. It is important to not power-cycle the unit during the download. Inbound and outbound traffic for mail continues when the update process is complete.

To check your subscription status:

1. Select **Basic** > **Status**.
2. In the Subscription Status section, verify the word *Current* appears next to Energize Updates and Replacement Service (if purchased). The following graphic shows the location of the Subscription Status section.
3. If the status of your subscription is Not Activated, do the following:

3a. Click the activate link as shown in the following example. This opens the product activation page.

3b. On the product activation page, fill in the required fields and click **Activate**. A confirmation page opens that displays the terms of your subscription.

3c. After a couple minutes, click **Refresh** in the Subscription Status section of the **Basic** > **Status** page. The status of your subscriptions should now be displayed as *Current.*

Note
If your subscription status does not change to Current, or if you have trouble filling out the product activation page, call Barracuda Networks at 1-888-ANTISPAM and ask for a sales representative.

Deployment Scenarios

The following diagrams have been provided to show some basic deployments. A brief description of some of the more major characteristics is also provided.

Non-DMZ

The first diagram depicts an installation of the Barracuda SSL VPN behind a firewall. Typically all port 443 (standard SSL port) traffic is routed through the firewall to the appliance. A proxy server could easily be included by placing it on the Internet facing side of the appliance should it be required. As the appliance simply sits behind the firewall all port 443 traffic passes through unchecked. This being the case care should be taken to ensure that unwanted traffic is dealt with correctly.

Within the DMZ

In this instance the Barracuda SSL VPN sits within the DMZ. Access is made through the firewall securely on port 443. Any access to resources on the trusted network requires another port to be opened on the firewall. This allows for traffic to reach the resource as there is no direct connection for the VPN to the internal network.

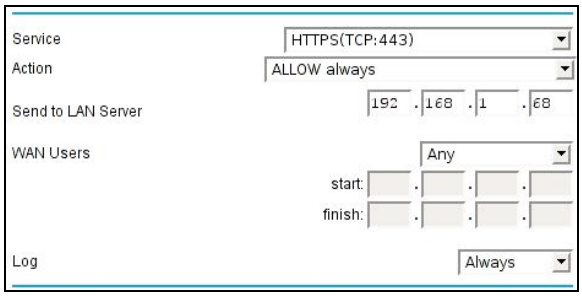
Configuring your Firewall to Route Incoming SSL Connections to the Barracuda SSL VPN

There are many implementations of firewalls using software or/and hardware to enforce an access policy. The way in which these rules are created can vary greatly. This being the case it may be necessary to consult the documentation accompanying the firewall being used.

The appliance requires the firewall to forward all SSL encrypted traffic to it in order to function correctly. This is achieved by adding a port forwarding rule (also known as a DNAT rule). Even though there is great variety with firewalls there will be a number of standard values required for the appliance to operate as expected. The following list shows some typical values required for a port forwarding rule:

- **Listening Port:** This is the port that the firewall will listen for SSL traffic. By default this is 443 but can be another value.
- **Target Port:** This is the port that all SSL traffic will be passed onto.
- **Target IP:** The IP address of the appliance is required here.

Below is an example of a simple firewall interface, the required values have already been filled.



Testing Connections to the Barracuda SSL VPN

It is recommended that a test be conducted to ensure that the Barracuda SSL VPN functions as expected. This is done by entering the URL or IP address of the appliance into a Web browser. For example:

- https://[IP Address]:[Port]
- https://www.mycomp.com:[Port]

If the connection attempt is successful then the following dialog will be presented.

Website Certified by an Unknown Authority
Unable to verify the identity of localhost as a trusted site.
Possible reasons for this error:
- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be localhost, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site localhost?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel

Seeing the above dialog means that the appliance has successfully been contacted and has sent a reply to the client's browser.

Appliance Administrator Web Interface

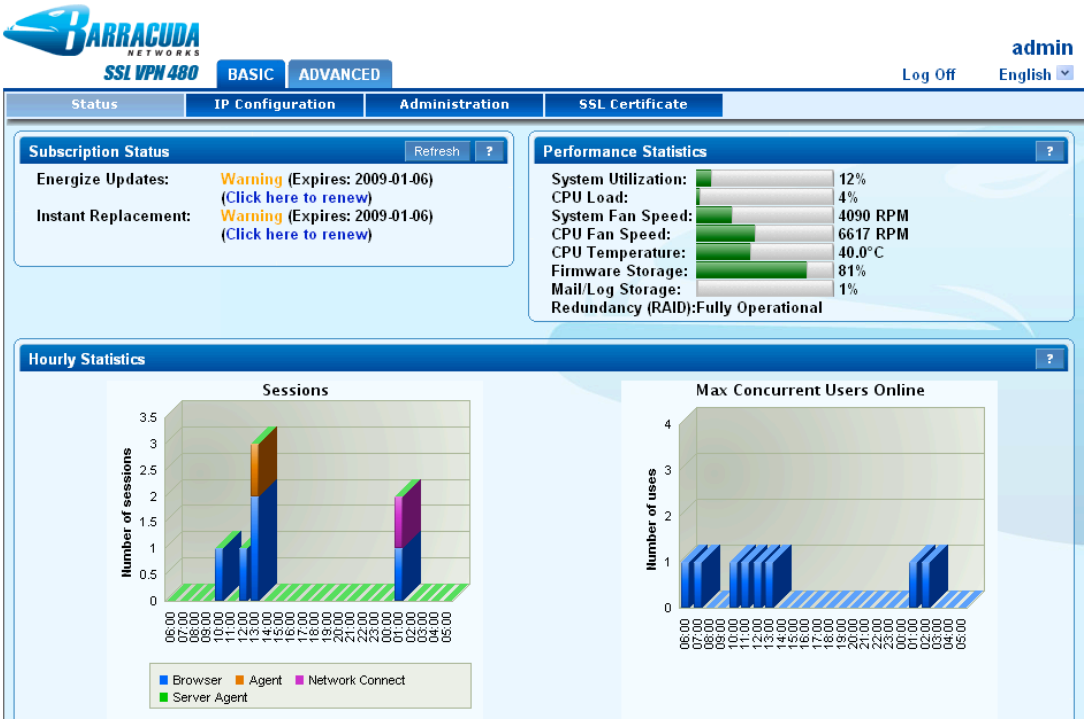
The Appliance Administrator Web interface is accessed using a different port to the standard interface and allows management of the hardware and other low level functions of the appliance. This includes such tasks as checking the status of Energize Updates, updating the firmware and configuring networking settings.

It is via the Appliance Administrator Web interface that the initial setup of the appliance is performed, along with other less frequently used maintenance tasks such as backing up the configuration.

The Appliance Administrator Web interface is accessed by connecting to your Barracuda SSL VPN using:

- **HTTP on port 8000**
- **HTTPS on port 8443**

To connect to the Barracuda SSL VPN via these non-standard ports you need to connect a browser to, e.g. http://yoursslvpn.com:8000 for HTTP, or https://yoursslvpn.com:8443 for HTTPS.



Monitoring the Barracuda SSL VPN

Checking Status

Check the **Basic > Status** page for an overview of the health and performance of your Barracuda SSL VPN, including:
• Active Sessions
• The subscription status of Energize Updates.
• System and hardware statistics, including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold.
• Incoming and outgoing throughput on the network interface.

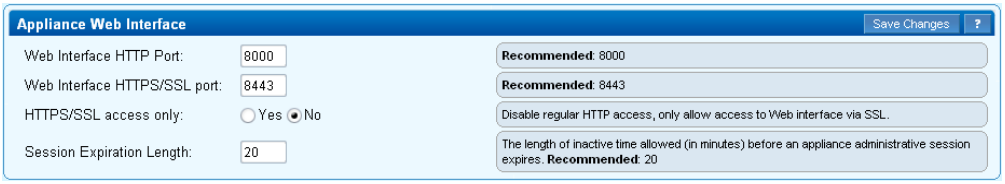
Viewing the Status Page Graphs

The following table describes the SSL VPN statistics displayed on the Status page. Note that some of these statistics are displayed in hourly and daily resolution.

Statistic	*Description*
Subscription Status	Shows the status of the Energize Updates and Instant Replacement service.
Performance Statistics	Displays information relating to the hardware in the Barracuda SSL VPN, such as CPU load and System Utilization.
Sessions	Displays the number of sessions active at any given time over the previous 24hrs
Max Concurrent Users Online	Displays the current number of users online and the maximum number of concurrent users that accessed the SSL VPN over the previous hour.
Received Throughput	Displays in bytes/sec the network throughput received on the network interface.
Sent Throughput	Displays in bytes/sec the network throughput sent on the network interface.

Configuring the Appliance Administrator Interface Ports

The default ports used for the Appliance Administrators Web interface are **8000** and **8443**; however these can be changed via the **Basic > Administration** page.



Configuring Network Information

Use the **Basic > IP Configuration** page to view or update the network settings for your Barracuda SSL VPN, including IP address for the LAN adapter, primary and secondary DNS servers and proxy server configuration.

Configuring an SSL Certificate

In order to only allow secured connections when accessing the Web administration interface, you need to supply a digital SSL certificate which will be stored on the Barracuda SSL VPN. This certificate is used as part of the connection process between client and server (in this case, a browser and the Web administration interface on the Barracuda SSL VPN). The certificate contains the server name, the trusted certificate authority, and the server's public encryption key.

The SSL certificate which you supply may be either private or trusted. A private, or self-signed, certificate provides strong encryption without the cost of purchasing a certificate from a trusted certificate authority (CA). However, the client Web browser will be unable to verify the authenticity of the certificate and a warning will be sent about the unverified certificate. To avoid this warning, download the Private Root Certificate and import it into each browser that accesses the Barracuda SSL VPN Web administration interface.

You may also use the default pre-loaded Barracuda Networks certificate. The client Web browser will display a warning because the hostname of this certificate is "barracuda.barracudanetworks.com" and it is not a trusted certificate. Because of this, access to the Web administration interface using the default certificate may be less secure.

A trusted certificate is a certificate signed by a trusted certificate authority (CA). The benefit of this certificate type is that the signed certificate is recognized by the browser as trusted, thus preventing the need for manual download of the Private Root Certificate.

Viewing System Tasks

Go to the **Advanced > Task Manager** page to see a list of tasks that are in the process of being performed and any errors encountered when performing these tasks. Some of these background tasks include firmware download and configuration restoration.

Backing up and Restoring Your System Configuration

Back up and restore the configuration of your Barracuda SSL VPN using the **Advanced > Backup** page. You should back up your system on a regular basis in case you need to restore this information on a replacement Barracuda SSL VPN or in the event your current system data becomes corrupt.

If you are restoring a backup file on a new Barracuda SSL VPN that is not configured, you need to assign your new system an IP address and DNS information on the **Basic > IP Configuration** page.

The following information is not included in the backup file:
- System password
- System IP information
- DNS information

Updating the Firmware of Your Barracuda SSL VPN

The **Advanced > Firmware Update** page allows you to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems.

In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version. If you have the latest firmware version already installed, the **Download Now** button will be disabled.

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours

Replacing a Failed System

Before you replace your Barracuda SSL VPN, use the tools provided on the **Advanced > Troubleshooting** page to try to resolve the problem.

In the event that a Barracuda SSL VPN fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call Technical Support and arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old Barracuda SSL VPN back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks Technical Support can provide details on the best way to return the unit.

Barracuda Networks
3175 S. Winchester Blvd.
Campbell, CA 95008

Reloading, Restarting, and Shutting Down the System

The **System Reload/Shutdown** section on the **Basic > Administration** page allows you to shutdown, restart, and reload system configuration on the Barracuda SSL VPN.

Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can also reboot the Barracuda SSL VPN by pressing **RESET** on the front panel of the Barracuda SSL VPN.

Do not press and hold the **RESET** button for more than a couple of seconds. Holding it for five seconds or longer changes the IP address of the system.

Using the Reset Button to Reset the LAN IP address

The Barracuda SSL VPN is assigned a default IP address of 192.168.200.200. You can change this IP address using the Appliance Administrators Interface (**Basic > IP Configuration**) or by pressing the **RESET** button on the front panel.

Pressing **RESET** for five seconds sets the LAN IP address to 192.168.200.200.

Pressing **RESET** eight seconds changes the LAN IP address to 192.168.1.200.

Pressing the button for 12 seconds changes the LAN IP address to 10.1.1.200. You will notice the three LEDs on the front panel flash at the same time intervals.

SSL VPN Administrator Web Interface

The SSL VPN Administrator interface is the main point of interaction between the administrators of the system and the system itself. This chapter introduces the reader to the SSL VPN Administrator interface and details its various functions. The sections included in this chapter are:

- Purpose
- Switching Views
- Accessibility

At the end of this chapter the reader should have an understanding of the management console and its purpose.

Purpose

The Barracuda SSL VPN is broken into three views – the Appliance Administrators Web Interface discussed in the previous chapter, the SSL VPN Administrator view and the SSL VPN User view which is the view displayed to the end users of the SSL VPN. The SSL VPN Administrator Web Interface view is known as the management console contains all the necessary functionality to manage the system.

From this console the user has the ability to create items that will affect users of the system whether that refers to a small group of users or the entire user base of the Barracuda SSL VPN..

Secure Access
Due to the system-wide effect of changes made through the management console, it is imperative that the console is accessible only by authorized administrators

Switching Views

The administration view is used by users with administration privileges to manage parts of the system while the user view is used to access resources within the company network.

To switch between views, select the appropriate view from the top right of the screen. Clicking 'Manage System' takes you to the SSL VPN Administrator view, and clicking 'Manage Account' returns you to the User view.

Accessibility

Initially only the administrator of the system will be able to access the management console. The administrator has access to every task and action available in the console and with this right is assigned the task of creating accounts for his administrative team.

In order to carry out administrative tasks as creating policies and users the administrative users must be assigned administrative control.

Users of the system mainly access the system via the user console to perform their daily tasks, accessing the internal network, creating application shortcuts, accessing internal files and documents in accordance with your access policies.

However this is not to say that a standard user of the system cannot access the management console. In fact as the above diagram shows, if given an appropriate **resource permission** a standard user will be able to access this console too.

Monitoring the Barracuda SSL VPN

Checking Status

When in the SSL VPN Administrator interface you will be presented with a different set of status page information. In this mode, the statistics returned relate to the SSL VPN statistics rather than those of the underlying hardware.

Viewing the Status Page Graphs

The following table describes the SSL VPN statistics displayed on the Status page:

Statistic	*Description*
Virus Scan History	Shows statistics relating to the virus scanning history on the SSL VPN.
Users Online	Statistics relating to the current number of VPN users online, including maximum numbers of users online since last restart.
Most Active Users	Displays a bar chart showing the users who have spent the most time using the Barracuda SSL VPN.
Most Popular Resources	Displays the most popular accessed resources, e.g. the specific web forwards or network places that have been accessed the most.
Sessions	Displays the number of sessions active at any given time over the previous 24hrs
Max Concurrent Users Online	Displays the current number of users online and the maximum number of concurrent users that accessed the SSL VPN over the previous hour.
Received Throughput	Displays in bytes/sec the network throughput received on the network interface.
Sent Throughput	Displays in bytes/sec the network throughput sent on the network interface.

Configuring User Databases

All user data used and managed by the appliance must be stored somewhere. The Barracuda SSL VPN allows the configuration of a number of databases to store this information.

By the end of this chapter the reader should have an understanding of each type of database and be able to configure the appropriate one that suits their particular requirements.

Configure User Database

The user database configuration page (**Management Console > Access Control > User Databases**) lists the available databases.

This page has the following properties:

- **Name:** The name to be associated with the user database.
- **Description:** A brief description of the user database.
- **User Database Host:** This property allows you to automatically select the user database that users authenticate against when connecting to the SSL VPN. When using multiple user databases you can enter here a hostname such as company1.example.com that is associated with the user database. A corresponding DNS entry should be made that maps this hostname to the Barracuda SSL VPN. When connections are made to the SSL VPN via this hostname, the user database to authenticate against will be automatically selected.
- **Show on logon page:** If this property is enabled, the new user database will be selectable in the logon page dropdown list box. If you do not wish users to be able to browse user databases other than their own, you can use this setting along with 'user database host' to auto-select the user database to authenticate against upon login.

Configuring the Built-in Database

Configuring the built-in database is very simple; just select the 'Built-in' option on the 'User Database Type' page. The appliance does all configuration of the database itself internally.

As this is a new database, once the appliance is up and running you will have to create all necessary users and groups from the management console. With the built-in database you will also be able to edit and remove users and roles directly.

Configuring Active Directory

Active Directory configuration is divided into three distinct tabs. The first of these is the connection tab.

The following information is required:

- **Domain Controller Hostname:** The primary Active Directory service domain in the form of, `example.barracuda.com`. The entry must be lowercase.
- **Backup Domain Controller Hostnames:** if backup domain controllers have been configured then these should be added here. This list should contain active controllers, which the appliance can fail over to in the event the primary domain controller is inaccessible. For more information on backup domain controllers refer to the section titled, Backup Domain

Controller. Hostnames can also be specified with a port number if different from the Domain Controller Port parameter.

Service Account Authentication
The standard Active Directory database uses GSS-API authentication for the service account. It is unable to authenticate credentials containing non-English characters. The service account does not need to be fully qualified.

- **Domain:** The domain the controllers are on for example, `example.barracuda.com`.
- **Service Account Username:** The service account details needed to use authenticate Active Directory users. You should configure a standard user account in Active Directory solely for the use of the Barracuda SSL VPN to query the directory.
- **Service Account Password:** The password to use for the service account.

Service Account
It is recommended that a specific AD user account be created for the Service Account only. This is required to support some of the other authentication methods available in the product.

The next tab OU Filter is an optional tab but allows specific organizational units to be added or removed.

- **Include Organizational Unit Filter:** Add any OUs that should be used when listing accounts and roles. Only the accounts residing in the OUs you specify will be shown. For further details refer to the section titled, Organizational Unit Filter.
- **Exclude Organizational Unit Filter:** Add any OUs that should not be used in the listing of accounts and roles.
- **Include Built-in groups:** This will include the default 'Built-in' group base `CN=Builtin` built from the domain name to the filter list.
- **Include distribution groups:** This will include the default 'Distribution' group base `CN=Distribution` built from the domain name to the filter list.
- **Include standard Users and groups:** This will include the default 'User' base `CN=Users` built from the domain name to the filter list. All users and groups under this will be added.

The final tab, Options, allows an advanced user the ability to fine tune access to the Active Directory database.

- **Service Authentication Type:** Which authentication method to use for server account authentication. GSS-API type is unable to process credentials which contain non-English characters but allows for the service account to be defined without full qualification. Simple authentication however is able to authenticate using non-standard character sets.
- **User Authentication Type:** Which authentication method to use for user account authentication.
- **Authentication Timeout:** How long the system should wait while authenticating
- **Authentication Maximum Retries:** How many times to retry to authenticate.
- **Connection timeout:** Generic connection timeout for active directory sessions
- **Cache Objects In Memory:** The system can cache user objects either to file or memory. If the user population is extremely large in-memory caching can be prone to running out of memory when loading objects.
- **Max Group Cache Objects:** The maximum number of group objects stored in cache.

- **Page Size:** The number of objects returned in each paged request, the default should be acceptable in most cases.
- **User/ Group Cache TTL:** This is the minimum 'Time to Live' value which must be greater than 10 seconds. Default value of 300 seconds stores Active Directory user information in cache for 5 minutes before clearing the cache. The next required action fetches user details again caching for another 300 seconds. A value too low will cause severe delays in processing any action as the appliance will continually be re-fetching data from the domain controller.
- **Member of Supported:** If the memberOf attribute supported on the user account, the groups are inspected to find the user's group associations. Note: Microsoft Small Business Server requires this to be unticked.
- **Enforce username case sensitivity:** This enables checking of username case sensitivity during log-on.
- **Follow Referrals:** Child domains require this value to be selected.

With the configured information the installation wizard will attempt to connect to the domain controller and valid the service account.

The wizard will allow the configured details to be adjusted before selecting **Next** again to retry.

Once a successful connection is made and the service account has been authenticated the Active Directory user database is ready to be used.

Configuring Enhanced Active Directory

Enhanced Active Directory configuration is very similar to the basic Active Directory configuration. It is divided into three distinct tabs.

The connections tab configures how to connect to the Microsoft Windows Active Directory service.

The only differing information for Enhanced Active Directory is the service account details.

- **Service Account DN:** The service account details needed to use authenticate Active Directory users. This account needs to be fully qualified e.g. `CN=John Smith, DC=Employees`.
- **Service Account Password:** The password for the service account.

Enhanced Active Directory database uses simple authentication for the service account. Simple authentication allows the use of non-standard character sets. With this type of authentication the account credentials need to be fully qualified.

The next tab OU Filter is an optional tab but allows specific organizational units to be added or removed.

The differing information here is the 'Group OU' information:

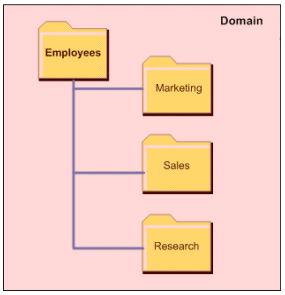
- **Create Group OU:** The OU location within the AD where new groups will be created.
- **Create User OU:** The OU location within the AD where new users will be created.

User Account Authentication uses Simple Authentication
Enhanced Active Directory uses Simple authentication for both the service account as well as user accounts.

Organizational Units (OUs)

In Active Directory, 'Organizational Units' (OUs) are the key structure for organizing users, computers, and other object information into a more easily understandable layout.

As the diagram below shows the organization structure has a root OU with three nested OUs below.



This nesting enables the organization to distribute users across multiple logical structures for easier administration of network resources.

When activated, the appliance takes the current Active Directory groups and maps them directly to groups.

The appliance also creates all internal data for each user within the chosen OUs. Each user will be assigned to the mapped roles.

Organizational Unit Filter

The Organizational Unit Filter makes adding OUs easier.

Entries in the filter must be of the form `'OU=<Organizational Unit name>'`. For example, `'OU=Research'`.

If an OU is held below another OU then the entire hierarchy up to the parent OU must be listed. If an OU called 'Marketing' was stored under the 'Employees' OU; to add 'Marketing' the correct syntax would be `'OU=Marketing, OU=User'` with the separating comma being used to separate each element in the hierarchy.

To add all OUs in the domain simply leave the Filters list box empty. When the list box is empty, all OUs will be queried. If problems are encountered with Active Directory, try clearing the list box.

To remove an OU from the search use the exclusion operator `#` against the OU name. For example to exclude the `Test Accounts` from the search you would add `#OU=Test Accounts`.

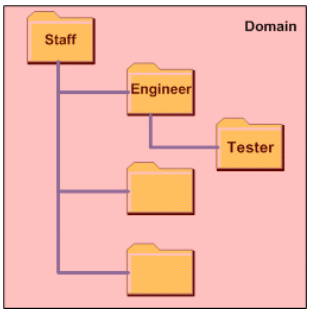
Troubleshooting

If your users are unable to connect via Active Directory, check that:

- The time settings between the Active Directory server and the Barracuda SSL VPN appliance are synchronized. Kerberos authentication, used by Windows, allows only a few minutes of clock skew between Windows server and client. Ensure that both the domain controller and the appliance are synchronized to the same date and time to within one minute.
- Confirm that the Windows server is configured for Active Directory authentication. If using Windows NT4.0 server, then the server only supports NT Domain authentication.

If OUs have not been loaded successfully:

- Any organizational units held within a tree structure need to be added with the entire parental structure.



In the above diagram to include '`Tester`' into the filters list the syntax should be '`OU=Tester,OU=Engineer,OU=Staff`'. The syntax begins with the lowest branch first.

- If any OUs are stored underneath the default Windows OU such as Users the '`OU=User`' root should not be included in the filter syntax.

- Check syntax of each filter. Every Organizational Unit must begin with '`OU=`'. If a hierarchy structure is being included, be sure to separate each element with a comma. Also avoid using unnecessary spacing.

- Clear the organizational unit filter to ensure that the entire Active Directory tree is searched.

Configuring LDAP

LDAP configuration is divided into five distinct areas. The first of these is the Configuration tab.

- **Hostname:** Hostname of the server hosting the LDAP service.
- **Port:** Listening port of LDAP service.
- **Protocol:** LDAP protocol to be used. Options include, secured 'SSL' communication or 'plain', unsecured communication.
- **Base DN of LDAP server:** The 'base DN' represents the location where you want to start LDAP queries within the namespace. This may be the root of the LDAP directory tree or a specific branch.
- **Service Account Authentication:** The LDAP authentication method required to access the service. The 'simple' method will require valid user account details to access the service; 'anonymous' will connect to the directory anonymously with no user credentials required and 'MD5-Digest' uses digest authentication to securely send the user credentials as an MD5 hash to the LDAP service as opposed to plain-text as with the other two methods.
- **Service Account DN:** The 'distinguished name' to identify the Service Account User.
- **Service Account Password:** The associated user password.

The next tab OU Filter is an optional tab but allows specific organizational units to be added or removed.

- **Create Role Organizational Unit:** The OU where new roles will be created.
- **Create User Organizational Unit:** The OU where new users will be created.
- **Include Organizational Unit Filter:** Add any OUs that should be used when listing accounts and roles. Only the accounts residing in the OUs you specify will be shown. For further details refer to the section titled, Organizational Unit Filter.
- **Exclude Organizational Unit Filter:** Add any OUs that should not be used in the listing of accounts and roles.

The next tab is the User Schema tab which provides schema information that the appliance can use to successfully link to the correct user classes at run time.

- **User class:** The LDAP class object used to represent a User class.
- **Username attribute: '**Username' attribute from the User class, if one exists.
- **Fullname attribute: '**Fullname' attribute from the User class, if one exists.

LDAP Class Objects
The Barracuda SSL VPN needs to understand which User and Role classes are in use by the given LDAP installation. Since each installation can use a different type of schema this information makes the appliance compatible with a larger number of LDAP installations.

- **Email attribute: '**Email' attribute from User class, if one exists.
- **Home directory attribute:** 'Home directory' attribute from the User class, if one exists.
- **Role membership attribute:** 'Role membership' attribute from the User class, if one exists.
- **Role membership contain DNs?:** If the 'role membership' attribute value points to a distinguished name then this box should be checked. The 'role membership' attribute can contain a value or otherwise refer to another object in the directory.

The next tab, ‘Role Schema’ requires role information so the appliance can successfully link to the correct role classes at run time.

- **Role class:** The LDAP class object used to represent a Role.
- **Rolename attribute:** The ‘rolename’ attribute from the Role class, if one exists.
- **Role membership attribute:** The ‘role membership’ attribute from the Role class, if one exists.
- **Role membership contains DN?:** If the ‘role membership’ attribute value points to a distinguished name then this box should be checked. The ‘role membership’ attribute can contain a value or otherwise refer to another object in the directory.

The final tab, Options, allows an advanced user to fine tune LDAP operations.

- **Connection timeout:** Generic connection timeout for Active Directory sessions.
- **Max Cache Objects:** Amount of information retrieved from the AD to cache. If the AD is large this should be set to a high value. Typically an object is cached for each user and one for each group. Calculating how many groups and users you have is a good guide when setting this. If the setting is too low some users may not be able to log in**.**
- **Page Size:** The number of objects returned in each paged request, the default should be acceptable in most cases.
- **User/ Group details Cache TTL:** This is the minimum ‘Time to Live’ value which must be greater than 10 seconds. Default value of 300 seconds stores Active Directory user information in cache for 5 minutes before clearing the cache. The next required action fetches user details again caching for another 300 seconds. A value too low will cause severe delays in processing any action as the appliance will continually be re-fetching data from the domain controller.

Configuring NIS User Database

There is one tab for the configuration of the UNIX user database:

- **Hostname:** The hostname of the UNIX server.
- **Domain name:** The UNIX domain name.
- **Refresh interval:** Remote account and groups are cached. This value is the interval (in minutes) between updates.
- **Include Local Accounts:** If selected, local accounts are also include in the list of available accounts. This only works on UNIX like system that have a /etc/passwd and or /etc/shadow file.
- **Include Local Groups:** If selected, local groups are also include in the list of available accounts. This only works on UNIX like system that have an /etc/group file.

Advanced System Configuration

The Advanced System Configuration (**Management Console → Advanced → Configuration**) page allows the configuration of various security related parameters. Security affects all areas of the system and so this page divides the configurable items into their respective areas.

User Interface

- **Allow Open Webfolder in Firefox:** When enabled, Firefox users will see the *Open As Webfolder* action for network places. This requires that the Open as Webfolder Firefox extension is installed
- **Maximum number of retrieved Users:** This property limits the number of users returned from a large user database for performance tuning.
- **Maximum number of retrieved Groups:** This property limits the number of groups returned from a large user database for performance tuning.

Web Server

- **Valid External Hostnames:** If a value is provided here, the hostname that the client uses to access the server must match one of those below. If it does not, the browser will be redirected to the first hostname in the list.
- **Invalid hostname action:** Sets the action to take if a client tries to connect using an invalid hostname.

Resources

- **WebDAV without cookies:** Allow WebDAV access from clients that do not support cookies. This would include Nautilus in Gnome, Finder in OS X and other WebDAV clients. Behaviour is much the same, except it is not possible to mount unauthenticated Network Places (i.e. those that would normally pop up a secondary authentication dialog). It may also have an affect on performance as authentication is performed on every request.

Network Places

- **Try current user (1st):** First, try using the current SSL VPN user / password if an underlying file store requests authentication.

- **Try guest (2nd):** Secondly, try using the underlying stores guest user and password if it requests authentication. This is store dependant.

Proxies

- **Non-Proxied Hosts:** Any host that should bypass the proxy server should be entered here. Entries should be one per line with no termination character. Wildcards such as '*.example.com' may be entered to exclude a range of hosts.

Web Forwards

- **Active DNS Host Format:** The format of the unique Active DNS hostname used to access reverse proxy web forwards.

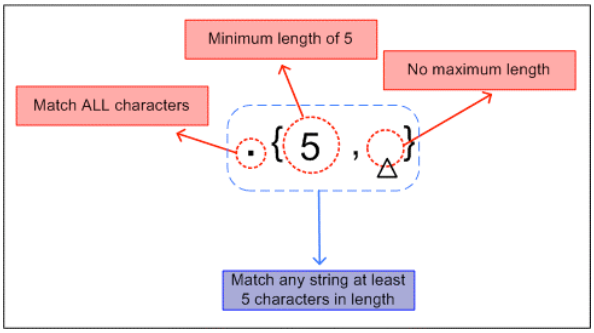
Password Options

This page contains all necessary information pertaining to the configuration of the password authentication module.

- **Max Logon Attempts Before Lock:** A value of zero disables this option; the default value is 3 logon attempts if after 3 attempts the account is temporarily locked.
- **Max Lock Attempts Before Disable:** The maximum number of temporary locks before the account is permanently disabled. Use a value of zero to never lock accounts.
- **Lock Duration:** The default value is 300 seconds; all values are in seconds.
- **Password Pattern:** The pattern that all passwords must match.
- **Password Pattern Description:** This description is shown to the user when defining a personal password.
- **Days before Expiry Warning:** The default value is 21, after which the warning will be displayed to the user informing them to change their password.
- **Days before Expiry:** The default is 28 days approximately one month after which the user will be forced to change password.

Password Pattern

The structure of an account password is based on regular expressions and is defaulted to, `.{5,}`, which defines a password with a minimum size of 5 characters. This expression is detailed in the diagram below:



The security function password structure is built around the 'regular expression' syntax. Any valid expression will be accepted to parse passwords an example is given below. Regular expressions are described in greater detail in Appendix A.

Expression	Meaning
X(n)	X exactly n number of times
X(n,m)	X between n and m
.[^\s]{n,m}	Any character except white spaces with a length between n-m
\w[n,m]	Word character [a-z,A-Z,_,0-9] between n-m

Session Options

Session options are security parameters used by the system to control how user sessions behave.

- **Maximum Logon Cookie Age:** Maximum age of the cookie that is used persist the logon if the browser is closed. A value of -1 will mean that the user will have to logon every time the browser is opened.
- **Multiple Sessions:** Defines whether the same user can log on multiple times. This option configures whether the same user is able to log into the system more than once simultaneously. The final 'Single Session per User / IP Address' is the most restrictive. This setting will prohibit the same user from accessing the Barracuda SSL VPN from two different locations simultaneously, locking down the user so that he or she can open a single session from a single machine.
- **Verify Client Address:** When checking logon state, verify the remote address of the request against the address recorded at logon. This prevents re-use of logon cookies from other clients.
- **Lock Session on Browser Close:** Enabling this option will force the user to provide their password upon opening a new browser and returning to the site.

Confidential Attributes

Confidential attributes are used by the system to store personal information about the user such as security questions which are used during authentication. These options configure how these attributes are encrypted.

- **Confidential Mode:** Determines how the passphrase for the user's private key is established. Attributes are stored by encrypting them with a user's public key so that they can only be decrypted by the corresponding private key. With automatic the passphrase for the private key is automatically configured as the users account password. If no account password has been provided then it will be prompted for instead. When set to Prompt the user will be prompted for the passphrase upon logon meaning that the passphrase will be independent of the user's password. Disabled will prevent the key being used at all, meaning confidential user attributes will not be encrypted at all.
- **Mask Personal Answers:** Checking this option hides the actual user responses with asterisk.

Appearance

Logon Page

This page defines the logon preferences. All users are affected by the changes made to this page.

- **Site Name:** Define a specific name for the site. When a user is presented with the logon page the title specified here is shown.
- **Welcome Text:** You can configure a custom title for the logon page. Leave this blank to use the default title
- **Message Type:** The type of message icon to show. This icon as well as the following message text I shown below the logon parameter.
- **Message Align:** Sets the alignment of the message text, options available are justify and center
- **Message:** The message you wish displayed beside the message type icon.

SSL Certificates

An SSL certificate can be configured for the purpose of encrypted communication between server and client. This page enables the management of this and other types of supported certificates. This chapter details the certificate related actions available to a user from importing new certificates and purchasing certificates.

SSL Certificates Interface

The SSL (Secure Sockets Layer) protocol is the standard method used in securing e-commerce transactions. SSL defines two methods for securing sensitive information during an SSL session they are encryption and authentication.

The page displays certificates related to each keystore type. As can be seen above, the keystore pull-down displays three different certificate types:

- **SSL VPN Server Certificate:** Certificates installed by the Barracuda SSL VPN for SSL encryption of VPN sessions. Browsers connecting to the appliance will receive this as proof of authenticity.
- **Trusted Server Certificates**: These certificates are usually provided beforehand by trusted vendors whose Web server the appliance may be expected to connect to at some point. The certificate contains a public key to allow the client and server to secure the communication.
- **Client Certificate Authentication:** This certificate is used by the client to authenticate itself with the appliance. The appliance creates this certificate containing a private key which is imported into the browser to authenticate itself with the server.
- **Server Authentication:** This certificate is used when the appliance, acting as a client, connects to another HTTPS server which requires authentication by the client through the use of a private key.

Action Icons

The action icons against each certificate perform functions on the associated certificate:

	Export certificate
	Export key

Certificate Actions

The action panel on the right of the page shows the actions that can be performed:

- **Import Certificate or Key:** Any further additions to the certificate database are imported from this option.
- **Download CSR:** Downloads the Certificate Signing Request for the server SSL certificate currently in use in order to be sent to a CA for signing.
- **Create CA:** Create a new authority

Creating a CA

A Certificate Authority is required to be able to issue certificates to the clients. This process defines the appliance as the authority to be able to issue and validate the client certificates that will be used to log into the server.

An external authority can also be used; the only thing required is the importing of the private key part of the certificates issued by this authority for each client so that the appliance is able to identify each client certificate being used to login with.

Step 1 From the Action menu select the **Create CA** action.

For a server which already has a CA, this step will be replaced by the **Reset CA** action. In this situation the CA does not have to be reinitialized each time.

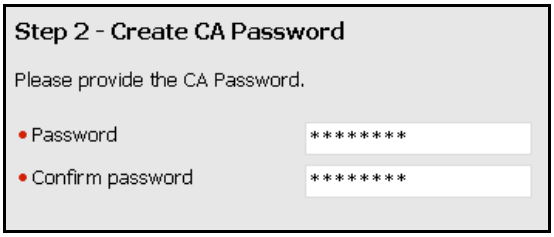
Step 2 This action loads the Create CA wizard. This wizard guides the user through the steps required to configure a CA for the system. Each certificate created for a user will be issued by this authority.

The information must all be completed. The information is then used to create a valid authority. The stamp of authenticity is all based around the content that is provided here, it is recommended that correct information be supplied.

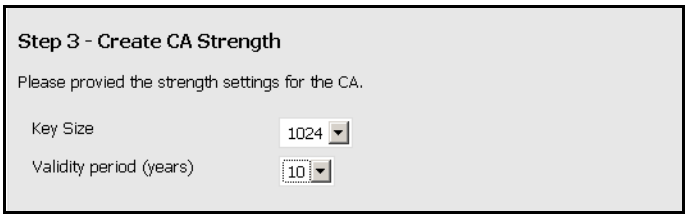
The required information and their meaning are detailed below.

- **Common Name:** The name the certificate should be referred to.
- **Location:** Where the authority is based
- **Organizational Unit:** The department of the authority
- **Company:** The name of the company or entity to which the certificate should be registered.

Step 3 To encrypt this information and the subsequent generated private keys the certificate requires an encrypting password.



Step 4 The strength of the private keys is next required. The larger the size the more complex the keys.

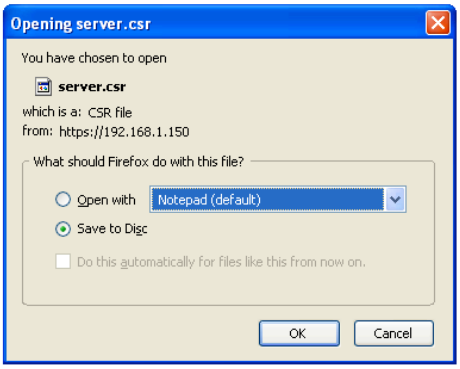


Step 5 Finally a summary I shown of the certificate that is about to be created. Pressing the **Finish** button will create the certificate else the **Previous** button will go back to each step and allow amendments to take place.

The newly generated authority will now be used to issue all client certificates. Generating a CSR

Step 1 Select the 'Download CSR' option available in the Action pane.

Step 2 The 'Download CSR' action takes the content from the unsigned certificate currently in use and produces a CSR. When ready the system makes the CSR available for download.



The file should be saved.

Importing a Certificate

Step 1 Select 'Import Certificate or Key' from the Action menu.

Step 2 Next, select the 'Input Type'. The appliance is able to import several types of certificate or key:

- **A reply from a certification authority:** A DER encoded certificate from a vendor.
- **A root certificate for your Web server's CA:** A root certificate to authenticate the issuer of your installed certificate.
- **A certificate from a server you wish to trust:** Add a specific server's signed certificate to the CA certificate trust store to trust the server.
- **A key for a server that requires client certificate authentication:** A private key to perform client authentication on outgoing connections in either PKCS2 or JKS format.
- **A CA certificate for verifying Active Directory user certificates:** A certificate from a CA used to authenticate Active Directory users.
- **A certificate you trust for client certificate authentication:** Only the Super User can generate internal certificates, use Active Directory certificates or trust a certificate. Importing a certificate through this option will trust a certificate for use with client authentication.

Step 3 Load the appropriate file.

Step 2 - File
Please choose the file you wish to upload as your certificate or key. If it is a private key you may be required to enter a passphrase as well. Depending on the type of import you may also be required to enter a name (or alias).
A certificate purchased from 3SP.com
Filename:
Y:\server.zip
Browse...
Previous
Next

Step 4 The system provides a summary of the action about to be performed. Selecting **Back** will allow the details to be modified.

Once completed successfully the newly imported certificate will be visible from the main SSL certificate page.

Exporting Keys and Certificates

If you need to retrieve the certificate or key for one that has been previously created then these can be exported again from the system through the export actions available against each certificate. For example if a certificate for an account has been lost then using these actions the certificate can be retrieved.

To export a certificate simply select the export certificate action associated with the certificate.

To export the associated private key, select the export private key action.

Attributes

As with any large user management system, functionality that allows for simpler administration is always welcome. User attributes are a simple concept that allow for drastically reduced administration overhead. This chapter aims to details what user attributes are and how to make the best use of them.

What are Attributes?

User attributes are simply attributes that perform a similar function to 'environment variables', and can be created by a user and used throughout the system. The appliance comes with a set of default attributes that cannot be removed these are used by the Personal Details Authentication module.

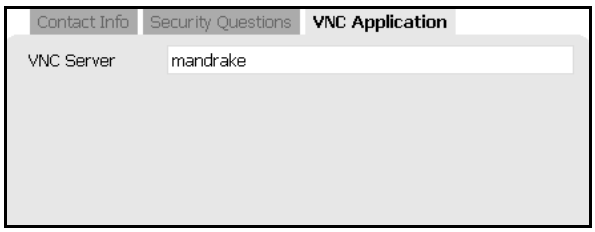
Security Questions

One of the default user attributes is placeOfBirth; all users have this attribute stored under the Security Questions tab (**User Console → My Account → Personal Details**). Each user can populate this attribute with their respective answer and when the Personal Details authentication module is used at log-on and asks a user for their place of birth, the module merely looks to the value stored under this attribute for each user logging into the system. If the attribute keyed in value matches that of the stored placeOfBirth value authentication is successful.

For each user logging in the respective attribute is compared allowing for a single attribute to be used by all users.

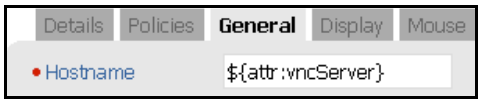
Applications

Attributes can be used with application shortcuts, an attribute can be created as below which defines a hostname and a port number.



Here the attribute VNC Server is a defined by each user, specifying which server they wish to connect to when using the VNC application shortcut.

The VNC application shortcut is configured to use this new attribute:

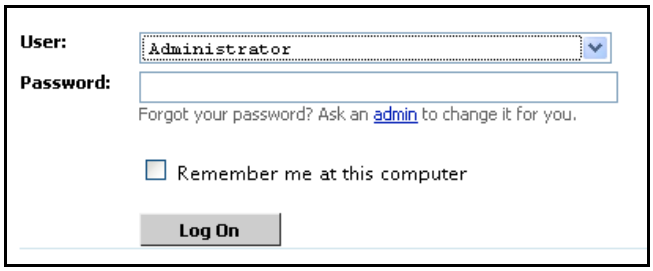


Whenever the application shortcut is executed, the system takes the current user's vncServer attribute and uses the value as the hostname to connect to.

Each user can define their own vncServer attribute to point to whichever server they wish to connect to. Thus for every user the application shortcut works differently, connecting to a different server without any further modification.

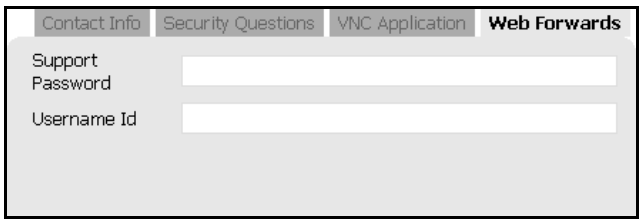
Web Forwards

The flexibility of user attributes also means they can be used in Web forwards. An example is a Web Site such as a support site which requires a form to authenticate users.

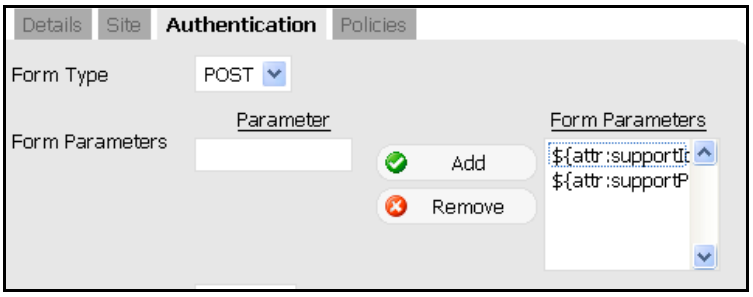


A standard username attribute cannot be used as the FORM has a drop-down list for user as opposed to a text field.

So here a user attributes is defined which specifies the associated user's ID. Two new attributes are defined which are confidential to the user only and specify the Username Id for the user and their password.



When the Web forward is configured the attributes are added to the authentication parameters.



When the Web forward is finally executed the supportId and supportPassword attributes are submitted during authentication into the Web Site. The FORM object takes the supportId and identifies the username then takes the supportPassword as the associated password.

Instantly any user is able to access the support Web Site using their credentials and this single Web forward.

Types of Attributes

The examples above all show the use of the user attribute where the attribute is assigned through the `${attr:attributeName}` command. There is also another attribute type called policy attribute. Unlike the user attribute which is assigned to each user this is assigned to a policy and is referenced by the `${policyAttributes:vncHostname}` variable.

Policy attributes once set are set for all users under the assigned policy. So a resource can be executed under a different policy and have a different value for each policy.

Attribute Interface

The screenshot below shows the user attributes main page accessible from **Management Console → Configuration → User Attribute.**

If you hover over an attribute (as with all resources) further information is shown in a pop-up:

- **Name:** Attribute name referenced wherever the attribute needs to be used
- **Label**: A more readable name for users to know what the attribute is for
- **Category**: Type of attribute and under what tab it should be stored in Personal Details
- **Visibility**: Whether the attribute can be managed by user or the administrator or both

Actions Icons

The action icon performs a particular function on the associated attribute. Available actions for a user defined attribute are:

	Delete User Attribute
	Edit User Attribute

Creating Attributes

Step 1 Select **Create User Attribute** from the action box at the top right of the page.

Step 2 The basic details of the attribute need to be completed first.

- **Name:** The name by which the system can reference the attribute.
- **Description:** Information about the attribute
- **Class:** Whether the attribute will be a user or policy based attribute.
    - **User:** User attributes become associated with users. Each user will need the value for this defined either by themselves or the super user
    - **Policy:** This attribute is attributed to a policy instead. The value defined for this will affect all users associated with the policy so this value only needs to be set once

Step 3 The attribute must now be defined.

- **Type:** The type of attribute.
- **Visibility:** The visibility of a user attribute is divided into 4 scopes:
    - **User or admin, use, view, override: T**his is the most relaxed level of visibility. Both the Super User as well as a user can fully manage the attribute
    - **User use and view, admin change:** Here the user is able to see the attribute, use it where necessary but cannot change the value associated with the attribute
    - **User use, admin view or change:** The user is restricted further by only being able to use the attribute managed solely by the Super User
    - **User Confidential:** The responsibility is reversed only the user has access to this, the Super User cannot manage nor visibly see this attribute
- **Label:** The name by which users can reference the attribute
- **Default Value:** The default value, depending on the visibility this value can be altered by the user or Super User.
- **Category:** The placement holder for the attribute, a new tab under **Personal Details** (**User Console → My Account → Personal Details**) is created with this value as its title.
- **Weight:** The order of where it should be placed in the category if there is more than one attribute under the same category. The higher the weight the lower down the list it will be shown. Weight is defaulted to 0 by placing an attribute at the top of the list.
- **Validation:** The validation class to use. The appliance comes with a set of default validators for each type of attribute. Some validators come with parameters that can be altered:
    - **StringValidator:** min and max length, trim blank spaces and even regEx or patterns can be used
    - **IntegerValidator:** min and max range values can be set
    - **BooleanValidator:** nothing can be defined, the validator checks for true or false only
- **Type Option:** You can also use this parameter to provide specific options to each type of attribute.
    - **Text:** for text attributes this parameter can be used to define the width that gets displayed.

- **Checkbox:** you can specify a replacement name for the default true, false values.
- **Text area:** this parameter allows the dimensions of the text area to be displayed. By specifying a number such as `30x2` will set the area to be 30 characters width by 4 lines height.

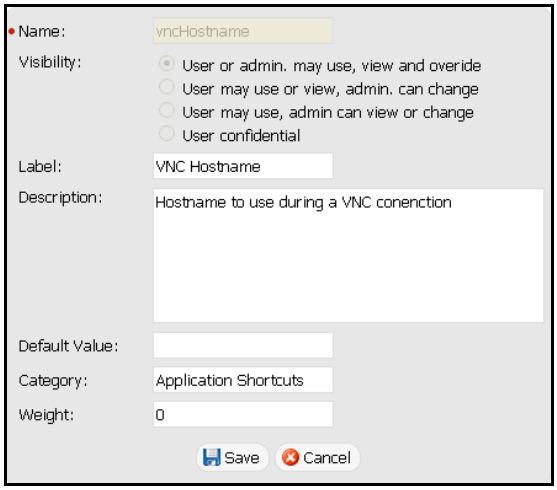
Step 4 Once complete, hitting the 'Finish' button will store the attribute and it will be accessible from the user attributes page.

If the attribute is a user attribute and set to be accessible by users then it will be available under **User Console → My Account → Attributes** under the tab also titled that of the defined category parameter.

If the attribute is a policy attribute then this will be visible under each policy. Editing a policy there will be a tab as titled in the category field or if this was left blank, under the default Attribute tab.

Editing an Attribute

From the user attributes page select the **Edit** action against the required attribute, the 'Edit User Attribute Definition' page will be shown. From this page the current details stored can be modified.



As the screenshot above shows the name cannot be changed.

Deleting an Attribute

The 'delete' action removes a user attribute permanently from the system. Selecting the **Delete** action against a user attribute will result in a warning message.

Selecting **Yes** will remove the attribute from the system.

Fixed System Attributes
User attributes created by the system such as those categorized under Security Questions are required by the system so cannot be removed nor edited; no available actions are associated with these.

How to use Attributes

Once a user attribute has been created it can be used throughout the system, wherever dynamic information can be loaded user attributes can be used.

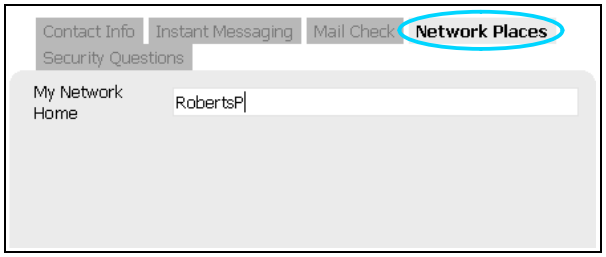
A user attribute is referenced via the `attr` command whilst a policy attribute is referenced by the `policyAttr` command. Below an example demonstrates how to set up a network place using user attributes.

Step 1 The user attribute 'myNetHome' is defined and stored under the 'Network Places' category.

Step 2 The network place is then defined.

As highlight in the screenshot shows the path uses the `${attr:myNetHome}` variable. When this is executed the system replaces the `${attr:myNetHome}` for the 'myNetHome' user attribute.

Step 3 Each user defines their 'Network Home' under the user attribute available from the Personal Details page. As the highlight shows the user attribute is available under the newly available Network Places tab as defined in the attribute definition page earlier.



That's all there is to it. Every time the network place is launched, the system dynamically takes the value of 'My Network Home' from the logged in user and replaces the `${attr:myNetHome}` parameter in the path. So for each user this will load their respective home share.

Session Variable

Another way to use dynamic parameters in the system is by using the `session` variable.
The session variable is used mainly when creating extensions, and it allows session information to be used and not user attributes.

With the above example we could also have used `session` as oppose to the `attr` variable like below.

The `session` variable refers to the values available during the course of the session. So as above the system would replace this with the username being used in this current session. This means that if the users home share on the network is named the same as the username used to log into the appliance (as might be the case in an Active Directory environment) then this Network Place will work and the home share of RobertsP would still be loaded.

The `session` variable can also be used to reference the user's password; so in an example of an application shortcut which requires both username and password we could use `session:username` and `session:password`.

More information on this variable and the available parameters that are accessible will be available in later releases of the documentation.

Access Control

This section details how the system can be accessed, from creating user account to giving users access rights to the system. Depending on what type of user database configured some functions are not accessible.

By the end of this chapter the reader should have a strong understanding of how the access control infrastructure of the product is built up and how it achieves such a strong level of access control flexibility.

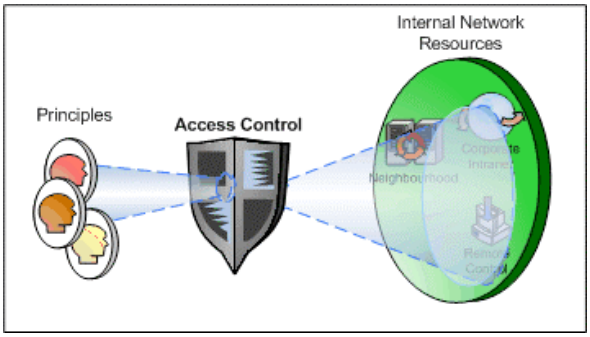
Introduction

This chapter covers a little access control theory as well as how the Barracuda SSL VPN deals with common challenges. It includes the following sections:

- Overview
- Access Control Architecture
- Flexibility

Overview

The Barracuda SSL VPN is a complete SSL VPN solution that provides secure, authenticated and controlled access to enterprise intranets, business applications and internal resources from virtually any modern desktop or notebook device.



At the heart of the product lies its access control engine. This is responsible for the complete management of all users from their initial log-on, right through to their exit from the system. More importantly it secures control of user access to different areas of the internal network.

The engine is the key component in verifying a user accessing the system and determining the actions that they may perform. Every action performed within the product is monitored by the access control engine in real-time and, as the diagram depicts, it acts as the 'guardian' of the system.

System of Trust

The concept of trust is a fundamental part of any secure system. As such it is crucial for the security policy to cater for and control how that trust is granted, used and revoked.

With trust playing such a significant part of remote access, the Barracuda SSL VPN solution has been designed to allow for either 'coarsely grained' or 'finely grained' access control. This approach allows the product to mirror more closely the actual trust relationships present in the real world. In conjunction with multi-tiered authentication schemes, our security model is much more advanced than those offered by conventional VPN solutions.

Levels of Trust

Trust is administered in measures - the more trust a user has the more privileges they are granted. Again the opposite is said for someone who has a lesser degree of trust and consequently is given a lesser level of ownership and access.

The Barracuda SSL VPN appliance follows this tried and tested pattern. With the access control framework, 'administrators' are seen as the most trusted users, seeing as they control the appliance. 'Power users' are given a lesser measure of control. Finally the standard user has a lesser degree of trust and therefore potentially the least level of access and responsibility.

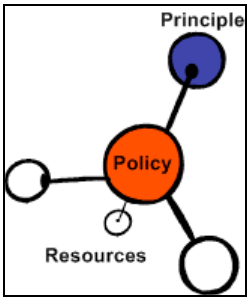
Access Control Architecture

The access control framework has been designed to tackle the following main issues.

- **Users and Groups:** Each organizations view on users and groups is almost always different. They do though share common behavior, e.g. 'Add User/Group' or 'Delete User/Group'. It is also likely that the organization's user/group directory already existed prior to the introduction of this appliance, for example an existing Active Directory domain or LDAP directory. The variety offered by such choice invariably gives rise to a number of different approaches and implementations.
- **Resource Access:** The intended outcome when implementing an SSL VPN solution is to allow remote access to network-based resources. The number of types of network resource is relatively varied and new methods are likely to appear. Each resource deployed can have very different access requirements, such as read or write permissions.
- **Resource Distribution:** A resource created within the system must be easily made accessible to those users that require it. Assigning resources on a per-user basis should be avoided wherever possible.
- **Resource Permissions:** Resources can have a range of permissions to limit how they may be assigned. When a resource is assigned to a user the user must be restricted to the set permissions. For example, a super user may create a resource to administer creation and assignment of application shortcuts only. This is assigned to a user who attempts to delete an existing application shortcut, this operation will be declined.

In order to resolve the aforementioned issues the access control architecture relies on three key entities:

- **Principal:** The intended 'consumer' of the resources, i.e. a user or a group.
- **Resource:** The networked resource, internal function or property item that the principal wishes to utilize, e.g. a Web-forward or the right to manage accounts.
- **Policy:** This is the relationship defined between the principal and resource. It is the component that ensures that only the right people can perform the right action.



Utilizing this methodology, the Barracuda SSL VPN is able to maintain robust, secure, and flexible access control architecture.

What is a Resource?

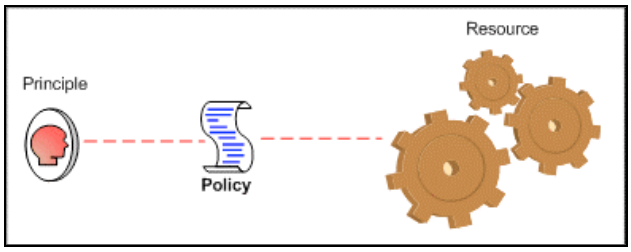
A 'resource' is defined as an application, utility, data source, or any other privileged ability that when assigned will allow the user to conduct certain tasks. Think of it as the endpoint, or objective that a user wishes to achieve. This could be something as simple as a user accessing their email client to read their mail. In this case, the resource would be the email. Similarly, an intranet Web Site would also be classed as a resource – just as a network share would be. All accessible stores of 'informational value' are deemed to be resources under this concept.

What is a Principal?

As already mentioned, the 'principal' simply refers to a user or group of users. The principal entity sits at the other end of the access control chain. The process flow begins with this entity and ends with the resource entity. Within the product these principals are only differentiated by the access rights they are assigned.

What is a Policy?

A 'policy' is the glue by which all principals and resources can cohesively work together. As the diagram below shows, the means by which a principal entity has access to a resource entity is through the policy and the means by which a resource entity becomes accessible is again through the policy.



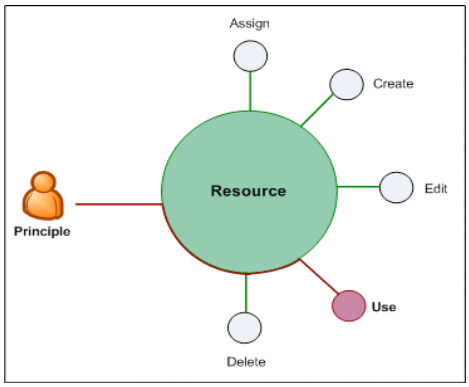
Policies represent a form of trust. A high level of trust equates to a policy of greater flexibility and responsibility; whereas a user with minimal trust may be assigned policies that grant them fewer privileges.

A 'power user' of the system manages the appliance and thus must have a higher degree of trust and consequently is granted a policy that covers a much greater scope of responsibility. The opposite can be said for a standard user whose policy may only grant the bare essentials required to allow them to perform their duties.

What is Permission?

A ‘permission’ is a special part of a policy. It adds the final level of control to the access control framework. As we have seen, not only can we control what resources a principal can access, but with this sub-element we can add a lower-level layer to control exactly the functionality a user can perform on any given resource.

For example as the diagram below shows, the policy is associated with a resource but the permissions on the resource only permit the associated principal to use the resource despite the resource itself having further actions such as editing, assigning etc .



With permissions we are able to lock-down control to the actions of the resource itself.

Creating Accounts

Principals in their basic form refer to the users of the system upon which the services are delivered. Accounts are the means by which a principal is created within the system. An essential process in building a robust and flexible system is defining what your principal base is.

This chapter details further what principals are and how the appliance manages these entities.
By the end of this chapter the reader should have a sound understanding of principals and how to model their required principal architecture successfully.

Principal Types

Principals at their lowest level represent a user, a consumer of the system. This is simply a user that will access the system. This can be in the form of a standard remote user accessing the system to carry out their work, to a 'power user' that maintains the system and creates users and organizes access control etc.

Principals however go one step further than this definition by incorporating the concept of 'groups'– a collection of users gathered into a single entity due to some similarities.

More details on groups can be found in the chapter titled, 'Creating Groups'.

Administrator Account

The only default user embedded within the appliance is the administrator. If the user database has been defined as built-in the user has the choice of providing authentication information for this user. If however the selection is anything other than the built-in database, the appliance will load the defined user list from within the database and the administrator is expected to choose from this list.

All other accounts throughout the system's lifetime are created by this super user and their purpose defined by their attached policies.

Structured Account Network
A policy structure should be considered before creating any accounts. Categorizing accounts into policies as 'Administrators' or 'Guest' will encourage a more structured and organized system. This is often imperative as the user base grows.

The administrator however is not categorized as a standard user, in fact the administrator is classified as the administrator of the system only and not as a typical user. The administrators purpose is to perform configurations of the appliance and from then on the super user should delegate its responsibilities out to other users of the system through access rights (**Management Console** > **Access Control** >**Access Rights**).

Account Interface

The main accounts page provides information on all accounts present within the system.

Action Icons

The action icons against each account performs functions on the associated account, their respective objective is detailed below:

	Delete account
	Edit account details
	Enable account – only visible if account is disabled (More…)
	Disable account – only visible if account is enabled (More…)
	Unlock account after authentication failure (More…)

Unsupported Database
Actions as 'Create', 'Edit', 'Delete' will not be accessible if the chosen user databases does not support external modification by the Barracuda SSL VPN. To make such amendments the administrator must access the user database directly.

Create New Account

Step 1 If a new account can be created the action pane will display the 'Create New Account' action.

Step 2 The 'Create User Account' screen will be shown. The page requires certain information to create the user, these are detailed below:

- **Username:** This field defines the name to be used to log into the system
- **Full name:** The name of the actual user responsible for this account. This name will be visible in the account summary page.
- **Email:** A contactable email address.
- **Enabled:** If checked, once the account has been given a useable policy the account will become active automatically.

Step 3 The created account can be assigned to a group. Enter the group name within the 'Group Name' field and use the 'add' and 'remove' buttons to associate the account with the given group. Further information on group selection can be found in the section titled, 'Assigning Groups'.

Step 4 Select **Save** to store the newly created account.

Cancellation of Account
Selecting the 'cancel' button will terminate the account being created. This can be pressed at anytime and no account will be added to the system.

Step 5 Once the account has been saved the system will ask for a password for the new account.

A new password must be entered. In addition the 'Force user to change password at next logon' setting ensures that the user make his or her password secure by forcing them to change it the first time they logon to the system.

Selecting **Save** will save the password against the new account.

The newly created account should be visible from the main Accounts page.

Assigning Groups

Groups are loaded by the system from the underlying user database. If the database supports modification to groups then the created account will be able to join a listed group.

For more information on which databases support group modification refer to the chapter in this document on 'Creating Groups'.

To add a user to a group with a user database that supports group modification, simply enter the name of the group in the 'Group Name' text box and select the 'Add' button. The group will then appear under the 'Selected Groups' list box.

If you wish to remove a user from a group, select the group name from the 'Selected Group' name list box. Pressing the 'remove' button will separate the user from the group .The name will also have been removed from the 'Selected Groups' list box. For more information on navigating the wizard refer to the chapter titled, 'System Navigation'.

Editing an Account

From the accounts page select the 'Edit' action against the required account and the 'Edit Account' page will be shown. From this page the current details stored about the account can be modified.

Deleting an Account

The 'delete' action removes a user permanently from the system. Selecting the 'delete' action against an account (from the accounts page) will result in a warning message informing that the user is about to be deleted. Selecting 'Yes' will result in the removal of the account from the system. If this user is associated with any policies these will also be removed along with all other associated links.

Creating Groups

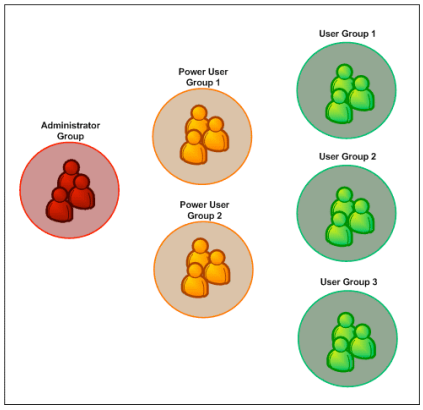
Groups represent the alternative type of principal. Groups offer a more convenient type for larger enterprises with a greater user base. This chapter details what a group represents and how they are utilized.

By the end of this chapter the reader should have a sound understanding of groups and how they can be used to provide structure to a user base.

What are Groups?

Principals define users in two forms: the singular being represented by a single account and the plural being a collection of accounts.

Groups allow for a more structured approach to account management; allowing an administrative user to categorize types of accounts under one heading as the diagram below shows.



Groups can be manipulated within the system as single entities but remember that all operations on the group will affect all accounts within the group. For example, an SSL tunnel resource can be linked to a single group and instantly every user within that group will be granted access to the attached resource.

Groups Interface

Action Icon

The action icons perform a particular function on the associated group. Available actions for a group are:

	Edit group
	Delete group

Create New Group

Step 1 If the user database allows for the inclusion of new databases then the 'Create New Group' action will be visible from the event pane on the right of the page.

Step 2 The 'Create Group' page will open.

The only detail required is the name of the group. If the supplied name already exists in the system an error message will be raised in the event pane.

Once a name has been defined simply add the accounts you wish to include in the group.

Selecting 'Create' will generate the group in the system for use. Selecting 'Cancel' will stop this operation.

If created the group should now be visible in the Group Page and can be used as any other group to assign accounts and policies to.

Editing a Group

From the group page select the 'Edit' action against the required group and the 'Edit Account' page will be shown. From this page the current details stored about the group can be modified.

Delete Group

Step 1 To remove an existing group, select the 'Delete' action associated with the group from the main group page.

Step 2 A warning message will appear.

To proceed with the removal of the group, simply select 'Yes'.

Creating Policies

Polices are the main building blocks in the access control architecture of the Barracuda SSL VPN. They form the bond between a principal and a resource. This chapter covers policies, from their purpose and usage to their unique characteristics.

By the end of this chapter the user should have a sound grasp of policy management and should be able to implement a structured policy framework.

What is a Policy?

On its own a policy is of little worth. However, by acting as a middle layer between two entities this makes it very powerful tool. On one side it is able to organize principals by a common goal(s) and on the other side it collates resources of a similar purpose. This approach helps provide order in a seemingly unstructured environment.

Principal Pool

A policy does not have to have a resource attached to it instantly. Policies in fact can also be used to simply group together a number of principals. As shown in the 'Example Policy Structure' section, the 'London Policy' is simply a holder of principals.

Stateless

A policy is linked to a resource and a principal. Both the resource and principal can be attached to any number of policies, there is no such thing as exclusivity. By this token any single resource or principal has no knowledge of any other resource or principal attached to the same policy.

Policy Interface

The policy screen displays a summary of available policies in the system. It is from this screen that we can create, edit and delete resources.

Action Icons

The action icon performs a particular function on the associated policy. Available actions for a policy are:

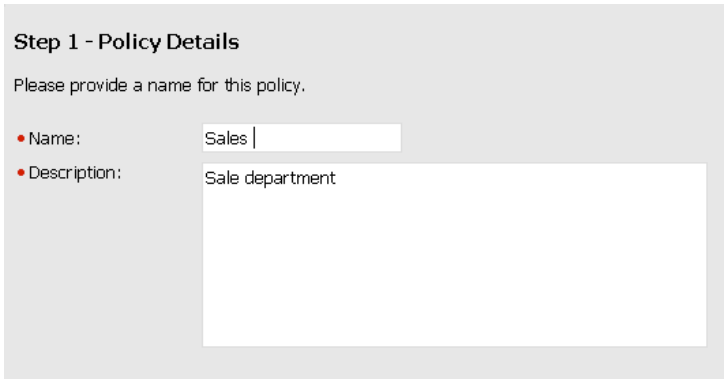
	Delete policy
	Edit policy details

Create Policy

Step 1 Selecting the 'Create New Policy' action from the event pane on the right will start the 'Create New Policy' wizard.

The system loads the 'Create Policy Wizard', and then the wizard guides the user through the steps required to create a policy successfully.

The wizard requires basic information relating to the policy to be created.



Required Information
Mandatory fields are marked with a red dot (●). Information must be entered for these fields.

The details required are listed below:

- **Name:** This required name will be displayed throughout the system. It will be seen and accessed by those with the right permissions so a sensible name should be used.
- **Description:** The description field helps to provide further information as to the purpose of the policy. It can be used to detail anything related to the policy and will be visible to others where necessary.

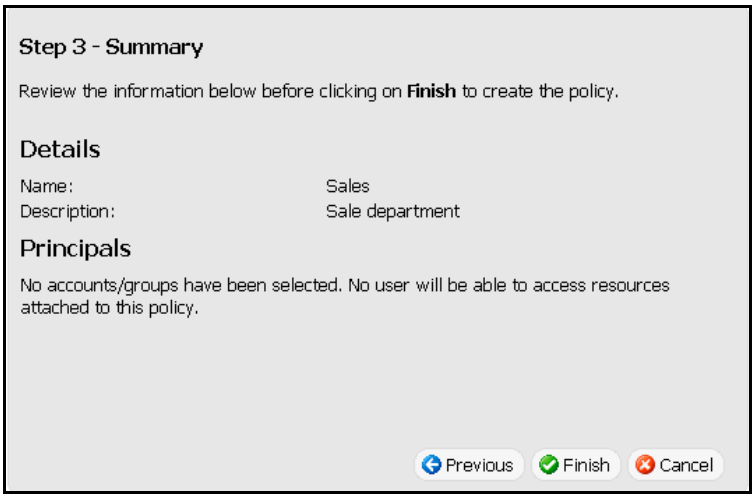
Step 2 As mentioned earlier, a policy binds principals to resources. The next step in the wizard allows the administrator to select those principals that will be associated to the new policy.

To add an account simply use the selection buttons; 'Add' to add an Account to the 'Selected Accounts' list box or 'Remove' to remove an Account. More details on this selection process can be found in the section titled, 'System Navigation.'

If the system's user database supports groups then these too can be added in the same way as accounts. For more information on groups please refer to the chapter titled, 'Creating Groups'.

Principals are Not Mandatory
A policy by default is made up of resource(s) and principal(s) but neither is compulsory. Policies can be created without any principals defined and if the user so wishes these can be added later in the 'Edit Policy' page. Also, policies do not necessarily require resources either. If the need arises, policies may be used for the simple purpose of logically grouping principals together.

Step 3 Before creating the policy the wizard provides a short summary.


Step 3 - Summary
Review the information below before clicking on Finish to create the policy.
Details
Name: Sales
Description: Sale department
Principals
No accounts/groups have been selected. No user will be able to access resources attached to this policy.
Previous
Finish
Cancel

If any of the details require modification then selecting the 'Previous' button will allow any previous step to be revisited and altered.

Once satisfied pressing the 'Finish' button will create the new policy. The new policy will now be accessible from the main 'Policy' page.

Editing a Policy

By selecting the 'Edit' action icon besides the policy of concern (from the policy page) the 'Edit Policy' page will be shown. From this page the current details stored can be modified.

Step 1 The tabs at the top of the page group the particular type of information, selecting each tab will allow you to modify the appropriate content.

Step 2 To save any new changes click the 'Save' button at the bottom right of the page. If you wish to discard changes simply select the 'Cancel' button.

Delete Policy

Step 1 To remove an existing policy, select the 'Delete' action associated with the policy from the policy page.

Step 2 A warning message will appear. To proceed with the removal of the policy, simply select 'Yes'.

Creating Access Rights

The final piece in the policy chain is the resource. Once a policy has been created and principals attached then these principals will require something to access – in this case a resource. Resources are defined in the system as two types. This chapter explains both types, detailing what they are and how to create these resources.

What is a Resource?

Within the Barracuda SSL VPN, a 'resource' is defined as an application, utility, data source, or any other privileged ability that when assigned will allow the user to conduct certain tasks. This could be something as simple as a user accessing their email client to read their mail. In this case, the resource would be the email.

What are Access Rights?

Access rights are essential in creating a well organized system. As mention earlier the super user should only be used to perform configuration of the system from then on the super user should create management users who are responsible for the daily uptake of the management and running of the system.

An access right allows the super user to delegate an area of responsibilities to a policy.

Nearly all areas of the system can be delegated to different policies thus allowing the super user to be disabled and not used other than for re-installation tasks or important configuration tasks.

All areas that can be managed are divided into their respective areas:

- **Resource Rights:** Items that can be managed in this area are all resources such as Web forwards, profiles and network places can all have their create, edit and delete actions delegated out to a policy.
- **System Rights:** Items that can be managed in this area that can be delegated are all system resources such as policies, SSL certificates, authentication schemes, accounts and auditing.
- **Personal Rights:** Items that can be managed here are all personal resources such as profiles, passwords, personal details, favorites and attributes.

Access Rights Interface

The access rights interface summarizes the currently available permissions.

The main page provides information on the resource permissions currently available.

Action Icons

The action icon performs a particular function on the associated resource permission; available actions are:

	Delete resource permission

	Edit resource permission

Creating an Access Right

Step 1 Select the type of access right from the action box. The wizard guides the user through the steps required to create a resource entity in the system.

Step 2 The first step in the wizard is detailing basic information pertaining to the resource to be created.

Required Information
Mandatory fields are marked with a red dot (●). Information must be entered for these fields.

The details required are listed below:

- **Name:** This required name will be displayed throughout the system. It will be seen and accessed by those with the right permissions and therefore a sensible naming convention should be used.
- **Description:** The description field helps to provide further information to the purpose of the resource. It can be used to detail anything related to the resource and will be visible to others where necessary.

Step 3 Resource permission simply defines what resources a user can access. Within this step the page allows the user to do just that. Clicking on the down arrow on the 'Resource type' reveals all the available personal resources that can be selected.

The first step is to select a resource from the list.

Once a resource has been selected **Add** those access rights you wish to provide permission to.

Step 4 As the policy structure states, a resource must belong to a policy. Without a policy the resource cannot be accessed or used. This step in the wizard requires a policy for which the resource is associated with.

Available polices are displayed to the left hand side and selected policies, which will have the resource assigned to them, to the right.

To add or remove policies simply highlight the policy in the appropriate box (to add select policies to the left, to remove, select policies to the right) and use the 'Add' and 'Remove' buttons.

Step 5 Before creating the resource the wizard provides a summary. If you wish to alter any of the details select the 'Previous' button to revisit and alter any steps.

Once satisfied pressing the 'Finish' button will create the new resource.

The new resource will now be visible and accessible from the main 'Resource Permissions' page.

Editing Access Rights

By selecting the 'Edit' action icon against a resource permission, the 'Edit Resource Permission' page will be shown. From this page the current details stored can be modified.

Step 1 The tabs at the top of the page group the particular type of information that can be edited; selecting each tab will allow you to modify the appropriate content.

Step 2 To save any new changes click the 'Save' button at the bottom right of the page. If you wish to discard changes simply select the 'Cancel' button.

Delete Access Rights

Step 1 To remove existing resource permissions, select the 'Delete' action associated with the resource permission from the main resource permission page.

Step 2 A warning message will appear similar to the one below. To proceed with the removal of the policy, simply select 'Yes'.

Authentication Schemes

Authentication is the means of verifying a user's identity; this can be in the form of a password or a code\key. To allow for greater security the Barracuda SSL VPN uses authentication schemes to provide a multiple staged authentication process. This chapter details authentication schemes, their purpose and how to implement a scheme.

By the end of this chapter the reader should have a sound understanding of authentication schemes and how to implement a necessary scheme to meet their requirements.

What is an Authentication Scheme?

An authentication scheme is simply a container for any number of authentication modules, such as OTP, Passwords, and Certificates. This approach means that multi-tiered authentication can easily be implemented and even linked to existing authentication systems. The authentication scheme is then used as the basis of the logon policy. The Barracuda SSL VPN allows for more than one of these schemes to be created and used.

It is important to note that certain authentication modules can only be used by themselves that is they cannot be combined with other authentication modules. The following section titled Authentication Modules describes any limitations pertinent to a module if any should occur.

When a user starts the authentication process they first have to enter a User ID. Once the User ID is submitted, checks are made to determine the correct authentication method to be used. This approach allows for different authentication methods to be used for different groups of users. For example users attached to a Sales policy may only have to enter a User ID and password, whereas Sales Management may be attached to a policy that uses a password and PIN authentication scheme.

The built in authentication schemes allow those wanting to build a single, double or even a triple factored process to do so with ease. All authentication schemes defined are visible from the authentication scheme page. Each of the schemes is listed in its order of priority.

Action Icons

	Delete policy
	Edit policy details
	Enable scheme
	Disable scheme
	Decrease priority of scheme
	Increase priority of scheme

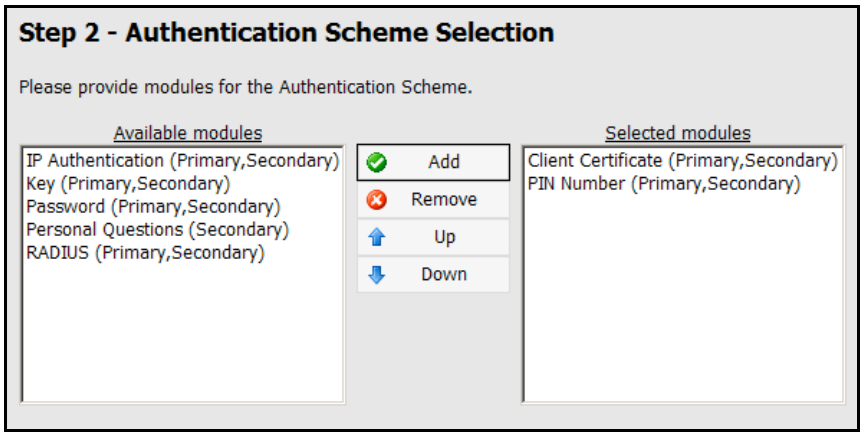
Creating an Authentication Scheme

For this example we will create a three-tiered authentication process. It will be a scheme using the Password module as a primary method, then PIN and finally Personal Questions.

Step 1 From the Authentication Scheme page select the only available action **Create Scheme**

Step 2 This starts the authentication scheme wizard. The first step in the wizard is defining the name for the scheme its description as well as its priority. The priority value can be from 1 to 9999 and indicates the order in which a scheme is to be handled. The lower the value the higher the priority.

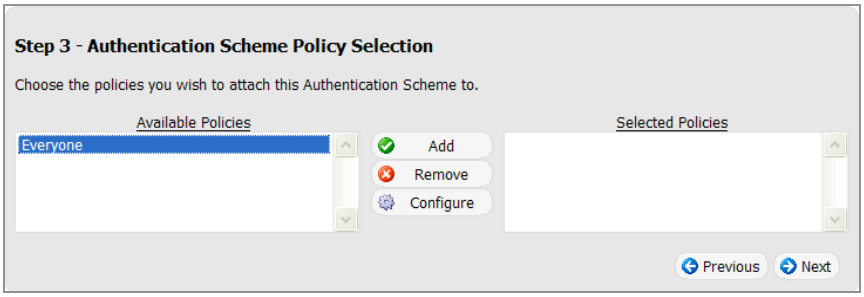
Step 3 Next the modules required for the scheme must be chosen. From the left pane all installed authentication modules are listed. Once an appropriate scheme is found press the **Add** button and the module will be added to the list on the right. This process should be completed until all the necessary modules have been added to the Selected Modules pane.



To reorder the modules chosen simply use the **Up** and **Down** buttons to adjust the order of a module.

Topmost Module Must be a Primary Module
At the top of the Selected Modules window there must be a module which can be a primary module. The system will not allow a scheme to be defined which does not have a primary module at the top of the list.

Step 4 An authentication scheme needs to be attached to a policy. This restricts which users can actually access the scheme.



Step 5 The final step is the summary. The system presents the details provided. If you are happy with the details pressing Finish button will result in the creation of the scheme.

The scheme will be visible from the main page. However the authentication scheme itself will not be available at logon. Instead the scheme needs to be enabled.

Simply press the enable action besides the new scheme.

An enabled scheme will have the enable icon besides it:

Whereas a disabled scheme will have the disabled icon besides it:

Deleting an Authentication Scheme

To remove an existing scheme, select the **Delete** action associated with the restriction from the main page.

Authentication Modules

As mentioned previously, there are differences in the level of control available for the configuration of a module. This section describes each of the modules.

Authentication	Type
Password	Primary/ Secondary
Client Certificate	Primary/ Secondary
IP	Primary
Authentication Key	Primary/ Secondary
PIN Number	Primary/ Secondary
Personal Questions	Secondary
OTP (One Time Password)	Secondary
RADIUS	Primary/ Secondary

The above table also shows what type an authentication module is. Type defines the order of the associated module. A primary module defines that the authentication module is capable of accepting a username and thus these types of modules should be placed first. Any module which has 'primary/ secondary' type can be placed as a primary module or a secondary module but any module which is strictly typed as, 'secondary' cannot be placed first in a scheme.

The authentication scheme system enforces this by disallowing a secondary scheme to be positioned at the top of the chain.

A brief summary of the available modules is listed in the following sections.

Password Authentication

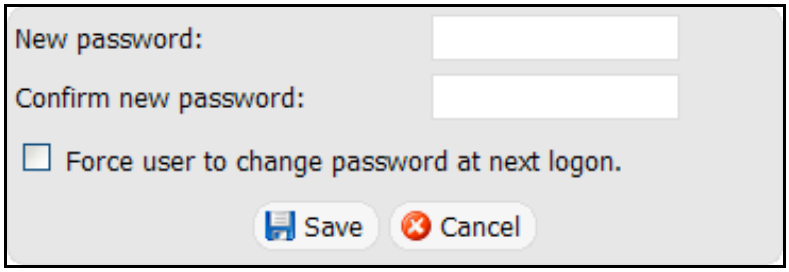
This is the most commonly used authentication scheme and it is the simplest and easiest to configure.

Both Default and Password and Personal Details rely on the Password authentication module; the first as a single scheme the second as part of a two-factor scheme.

The length, format and expiration of passwords are all configurable, however initially these parameters are defaulted and whenever the administrator creates an account a password must be attached.

Creating a Password

A password is assigned the first time a user is created. As the screenshot below shows the password can be redefined the first time the user logs into the system by selecting the checkbox.



For further information on creating passwords refer to the chapter titled, Creating Accounts.

Modifying a Password

Once a password has been assigned to the account it can be altered at any time by both the administrator from the Management Console and by the user through the User Console.

Management Console

Step 1 Choose the account you wish to edit from the Accounts page (**Management Console** > **Access Control** > **Accounts**) by selecting the associated '**More…'** button.

Step 2 A new set of actions becomes available. Selecting **Set Password** allows the administrator to change the password for the account.

Step 3 From here a new password can be defined. In addition the checkbox at the bottom can be selected to force the user to change their own password when they next log in.

User Console

This method is used by the user allowing them to securely modify their own password without any intervention by the administrator.

Step 1 From the My Accounts section select **Change Password**.

Step 2 The user is now able to change their password from the Change Password page.

The user is expected to key in the original password as well before the change can occur.

By default the system will lock any user that fails authentication after three attempts and again disables any user who has been locked out three times consecutively. These parameters are configurable and are detailed in the section below.

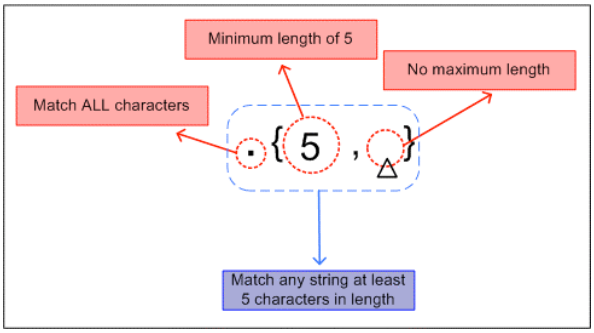
Configuring Passwords

The configuration options can be accessed from **Management Console** > **Advanced** > **Configuration** > **Password Options**. There are a considerable number of parameters that should be understood as the Password authentication module is commonly used as the default authentication scheme and tends to be found in most other multi-factored schemes. The configuration parameters are detailed below:

- **Max Logon Attempts Before Lock:** A value of zero disables this option; the default value is 3 logon attempts, if after 3 attempts the account is temporarily locked.
- **Max Locks Attempts before Lock:** A value of zero disables this option; the default is 3 temporary locks, after which the account is permanently locked.
- **Lock Duration:** The length of time an account is locked; default value is 300 seconds.
- **Password Pattern:** The definition of a password, how passwords should be constructed. Details on Password patterns can be found below.
- **Password Pattern Description:** This description is shown to the user when defining a personal password.
- **Days before Expiry Warning:** The default value is 21, after which the warning will be displayed to the user informing them to change their password.
- **Days before Expiry:** The default is 28 days approximately one month after which the user will be forced to change password.

Password Pattern

The structure of an account password is based on regular expressions and is defaulted to, `.{5,}`, which defines a password with a minimum size of 5 characters. This expression is detailed in the diagram below:



The security function password structure is built around 'regular expression' syntax. Any valid expression will be accepted to parse passwords an example is given below:

Expression	Meaning
X(n)	X exactly n number of times
X(n,m)	X between n and m
.[^\s]{n,m}	Any character except white spaces with a length between n-m
\w[n,m]	Word character [a-z,A-Z,_,0-9] between n-m

Personal Questions Authentication

This is another commonly used authentication module. Its simplicity and ease of use make this a favorite choice amongst multi-factored schemes. In fact much like Password authentication, Personal questions is also part of the default set of authentication schemes.

Since this is a secondary-only module it is the second stage module in the Password and Personal Details scheme.

Personal authentication relies on pre-defined personal information about the user. A set number of questions are managed by the system and when utilized the system takes a question and presents this to the user. A comparison is made between the current answer and the preset answer; if a match is made the user is authenticated.

This authentication method is a secondary option only and must work in conjunction with a more secure module.

These cannot be amended nor can a user add additional question to these.

Configuring Answers

Both the administrator and the user are able to configure answers for these questions through the Management Console and User Console respectively, but it mainly falls within the responsibility of the user to provide secure and personal answers to each question, something that they will remember and secure enough so that no other user can guess. The steps involved in configuring these are minimal but have been detailed below nonetheless.

Management Console

The administrator can access the user's personal details and alter these details if so required.

Step 1 From the 'Accounts' page (**Management Console** > **Access Control** > **Accounts**) select the Edit action against the account to edit.

Step 2 From the Edit Account page select the **Security Questions** tab.

Step 3 This displays the available personal questions and where necessary populated with answers. These can be altered. When satisfied with the changes pressing the **Save** button will store the new answers.

User Console

It should be the user's responsibility to manage and update their personal details.

Step 1 Open the 'Edit Personal Details' page from **User Console** > **My Account** > **Personal Details**

Step 2 Select the **Security Questions** tab

Once all the answers have been supplied pressing the **Save** button will store these for use during authentication.

Resource Management

Resources are the key entities that a user of the system will interact with. Without such things, a user has no means of using or gaining any benefit from the system – it is the resources that provide the 'value' in an SSL VPN. This section covers the basics of resources; what they are, how they are used and finally ends with what types are available.

What are Resources?

The main purpose a user will use an SSL VPN is to access the corporate network usually from a remote site, be it from a remote branch office or from a clients site. Securely allowing users into your network is just one side of the remote access solution. Once logged in, the user must have a means of actually interacting with items within the corporate network such as network drives, files and applications and this is where resources fit into the picture.

Some resources such as Network Places allow a user to interact with shares on the network. Other resources as Web Forwards allow users to interact with company intranet Web Sites. Each resource provides a different way to access and interact with the remote network, from running remote applications to creating secure VPN tunnels.

It is the administrator's responsibility to create these resources and provide a secure working environment for the remote user population. Without the right configuration of resources, accessing areas of the corporate network remotely would be at the least difficult and in the worst case, impossible.

The administrator is also responsible for the management and configuration of resources. As the corporate network evolves so to must the resources which access the network. As further company security policies are put in place not only must the network change to suit but so too must the appliances resources.

The user console is the page from which the users are able to access these resources for use. Resources are listed under the **Resources** tab and these can also be added to a user's Favorite page. Administration of resources however is done through the Management Console.

Resource Wizards

Every resource is created through an intuitive wizard. The wizard directs the administrator in defining the appropriate steps in the correct order.

Some of these steps can be skipped and then redefined as required through the **Edit Resource** pages later. Also any step can be re-attempted by simply clicking on the appropriate step in the Navigation Pane.

Available Resources

The Barracuda SSL VPN defines a number of resources. Resources that can be used are listed below:

- **Web Forward:** Provides secure intranet and internet access

- **Network Place:** Provide network file system access
- **Application:** Deployment and execution of applications
- **SSL Tunnel:** Configure SSL tunnels for special tasks such as remote support
- **Profile:** User environment configuration
- **Barracuda Network Connector:** A virtual network adaptor that provides full TCP/IP into the network

Each chapter is dedicated to one of these resources covering everything from creating to managing the resource.

Executing a Resource

All executable resources follow a similar set of steps when being executed and these are detailed below.

Step 1 From the user console find the resource to execute. Against this resource will be the execute button

Step 2 When pressed the execute button needs a policy in which the resource should be executed. The execute button lists all the policies the resource is connected to, selecting one will execute the resource using any policy attributes associated with the chosen policy.

To execute a resource simply press the correct icon. The resource will execute in the first policy the user has been assigned to, usually everyone.

Step 3 The resource should now execute opening the required window if necessary.

The Barracuda SSL VPN Agent

Many commonly used applications typically operate using unsecured protocols to facilitate the exchange of data. To the casual home user this is usually not a worry, though to the corporate user this is a critical vulnerability and one that leaves a business open to all manner of threats from password sniffing to industrial espionage.

With modern encryption protocols like SSL, data from these applications can be "tunneled" inside SSL packets. In the Barracuda SSL VPN appliance this is achieved through the use of the SSL VPN Agent – a small program that can intercept data transmitted by the insecure application, encrypting said data and transmitting the secure form over the wire. At the receiving end the appliance decrypts this data and forwards it to the appropriate destination within the trusted network.

What is the Barracuda SSL VPN Agent?

With the Barracuda SSL VPN appliance comes a small SSL VPN Agent. This is a Java application that works in conjunction with your user session to provide SSL tunneling and application launching facilities provided by the appliance.

The Barracuda SSL VPN Agent is launched by a small Java applet placed on all pages that require access to the SSL VPN client. You only need to launch the client once per user session.

The Barracuda SSL VPN Agent is an essential tool for providing a secure tunnel for some of the resources detailed later in this chapter. When required the resources automatically starts the Agent. However the Agent can also be started manually in which case any resource requiring the use of the tunnel will not need to start the Agent.

Communication with Browser

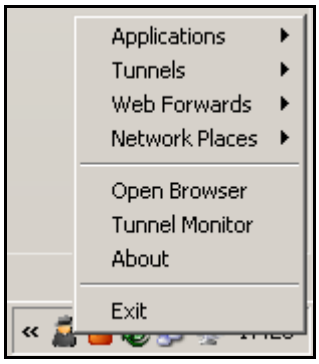
The Barracuda SSL VPN Agent listens on a number of ports in the 65500+ range. This is normal behavior. The Agent is actually also a HTTP server and uses these ports to communicate with your Web browser. All outbound network communications are sent through the HTTPS port 443.

Precautions

It is important to remember that the SSL VPN Agent will provide a secure tunnel into your network until it is closed or times out due to inactivity. Your users must make sure that they log-off from their SSL VPN sessions. It is not wise to allow such a session to remain open and unattended even for a short period of time. The SSL VPN Agent will time out any tunnel that is inactive for a configurable period of time.

Executing Resources from the Barracuda SSL VPN Agent

Once the Barracuda SSL VPN Agent is started you can execute any resource assigned to you from the directly from the taskbar icon. Clicking the right button the Agent icon will present a list of resources that can be executed directly from the Agent.



By opening the **Tunnel Monitor** one can view any tunnels that are created through the life of the Barracuda SSL VPN Agent. From here you can also kill any active tunnels.

Web Forwarding

Web forwards provide a secure way of remotely accessing a company's intranet resources and as such are an essential tool in helping reduce the risk of unauthorized access to the corporate network. This chapter covers all the essentials to allow a super user to manage these resources, from what a Web forward is, how they work to managing them. Web forwards come in three types - tunneled, path based reverse proxy and replacement proxy. This chapter details each and when best to use each type.

By the end of this chapter the reader should have a good understanding of Web forwards and how to use them.

What is a Web Forward?

Simply put, Web forwards redirect HTTP traffic. By creating a Web forward the publisher can make an internal Web resource accessible to the outside world – without ever having to publish the resource on to the World Wide Web.

Take for example a company intranet or an internal Web-based application. Without Web forwards users can only access these resources internally within the LAN. Trying to access these remotely would mean having to publish these on the Internet. Making a company's sensitive internal resources available over an un-trusted publicly accessible network leaves the system vulnerable to attacks.

Web forwards reduce these vulnerabilities by publishing Web forwards on a VPN. The elimination of the resource from the Internet instantly minimizes the chances of the internal network being compromised. When accessing the Web resource users have to sign in to the user portal through strict authentication techniques. During the course of the session the communication channels are secured through SSL and then to further enhance security your appliance's policy settings can restrict those that can even access the Web forward.

Technical Overview

The Barracuda SSL VPN provides four ways in which a Web forward can be created, and these are as follows:

- **Tunneled:** Suitable for static intranets, requires launch of the Barracuda SSL VPN Agent.
- **Replacement Proxy:** Suitable for Web applications which use absolute URLs with minimal JavaScript.
- **Host Based Reverse Proxy:** Suitable for Web applications which use relative URLs and tend to be more complex than those for replacement proxy.
- **Path Based Reverse Proxy:** Suitable for Web applications that do not exist at the root path of a Web server.

Each one is briefly described below.

Tunnelled Web Forwards

A tunneled Web forward uses the Barracuda SSL VPN Agent. If not already installed the Agent is downloaded to the client machine. The Agent acts as an Agent for the client browser handling all necessary transaction to provide a secure connection to the target resource. The communication link between browser and Agent is the only line that is not encrypted.

Unlike reverse and replacement Web forwards the content of the HTTP traffic are not altered at all. No content is changed from the moment it leaves the client to the response that is received, the Barracuda SSL VPN acts a dumb proxy providing no functionality. This Web forward performs the same functionality as a standard SSL tunnel.

The unique feature is that no content is processed. However if the target site has links to other sites and are selected then those pages will step out of the secure SSL tunnel boundary and will not be securely accessed.

Replacement Proxy Web Forwards

A replacement Web forward, unlike the tunneled forward, does not rely on the Barracuda SSL VPN Agent. Despite this the communication link both to and from the intranet resource remain encrypted due to the browser and the appliance.

The Barracuda SSL VPN retrieves the Web page on behalf of the connecting client. Information received by the appliance is processed by the replacement engine which is in stark contrast to the tunneled Web forward. The data is stripped of certain information and new information is added to the transmission, all links within the page are replaced to point back to the appliance. The transmission is then encrypted or left unencrypted depending on the target server HTTP/ HTTPS.

The responses are again preprocessed by the replacement engine before being securely sent back to the client.

This processing means that any additional links attached to the Web resource are handled by the Web forward. As long as the Web forward remains open all pages are processed and remain secure. So for example a Web application that opens up various pages or goes off to various other sites will continue to be processed by the forward.

Reverse Proxy

Reverse proxy like replacements does not rely on the Barracuda SSL VPN Agent and again despite this the communication link remains encrypted due to the browser and the appliance.

Unlike replacement Web forwards the content is neither altered from the moment it leaves the client to the response that is received, the appliance acts as a reverse proxy server for the target client.

Unfortunately if the target site has links to other sites and are selected then those pages will not be secured.

Web Forward Interface

The main Web forward page lists the available forwards. This page is located under **Management Console** > **Resources** > **Web Forwards**

The main page details which policy a Web forward is associated with, the type of the Web forward and the category of the Web forward.

Only those Web forwards associated with a user's policy are visible from the user console under **User Console** > **Resources** > **My Web Forwards**.

Action Icons

The action icons against each Web forward performs functions on the associated Web forward, their respective objective are detailed below:

	Delete Web forward
	Edit Web forward details
	Execute resource (User Console)

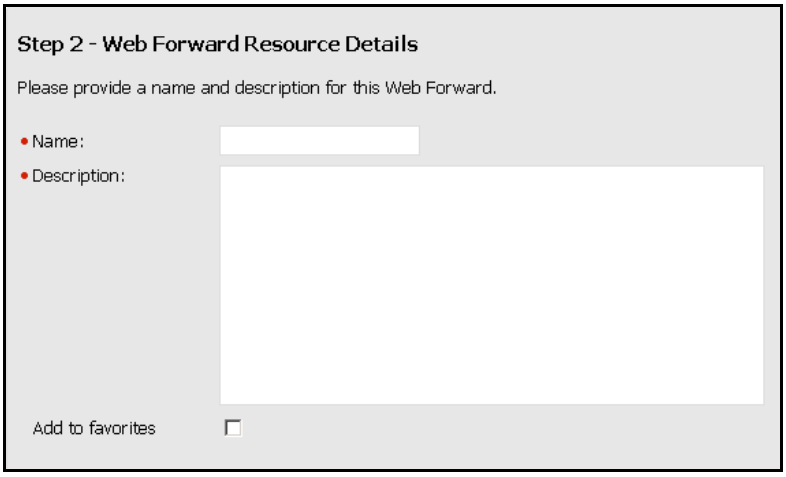
Creating a new Web Forward

Step 1 Select the Create Web Forward action.

Step 2 Select the type of Web forward you wish to create.

Step 3 Once selected the Web forward wizard will open. All Web forwards follow the same wizard process as below.

The first step in the wizard is to provide details of the resource itself, the name and description of the resource.


Step 2 - Web Forward Resource Details
Please provide a name and description for this Web Forward.
Name:
Description:
Add to favorites

The final Web forward can be set as a favorite resource which will make this resource accessible from the favorite's page.

Step 4 The second step defines the resource itself. For each Web forward the required content differs. These are detailed below.

Configuring a Tunneled Web Forward

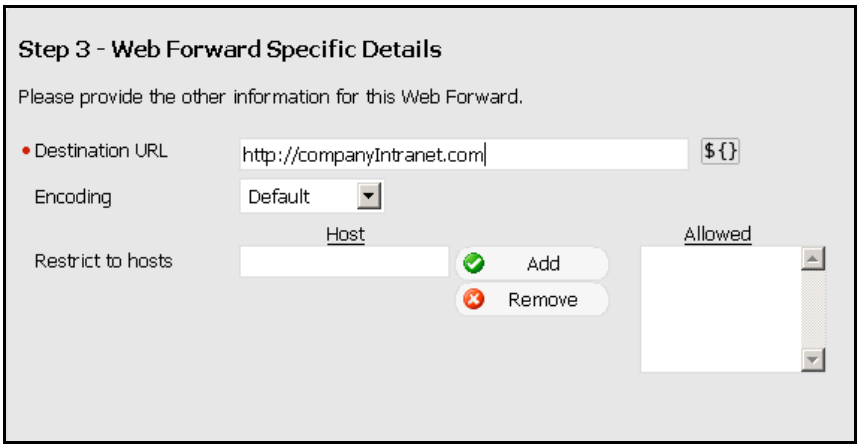
This Web forward requires the least amount of information. All the wizard requires is a valid URL the authentication step is skipped.

Step 3 - Web Forward Specific Details
Please provide the other information for this Web Forward.
Destination URL
http://companyIntranet.com
${}

The wizard provides a mechanism to use built-in system parameters these are detailed a little more in the **Create Replacement Proxy** step next.

Configuring a Replacement Proxy Web Forward

Replacement details require two sets of information; the first is the basic information of the Web site.



- **Destination URL:** The URL of the site you wish to access
- **Encoding:** This overrides the encoding of the HTTP response; this should be left as default unless otherwise informed by a Barracuda Central engineer.
- **Restrict to hosts:** This restricts what hostnames the user can access. Any user accessing the site can access only the URL hostname and any hostnames listed in this box. If the list is empty then no restrictions apply, if the hostname specified is the hostname of the URL then users cannot access any pages located outside of the hostname.

Note

Replacement Variables
The `${}` indicates that replacement variables can be included in the resource definition. Click this icon will load the available variables that can be used. The `session` variables are values taken from the current session. The `attr` variables are values taken from user-defined attributes.

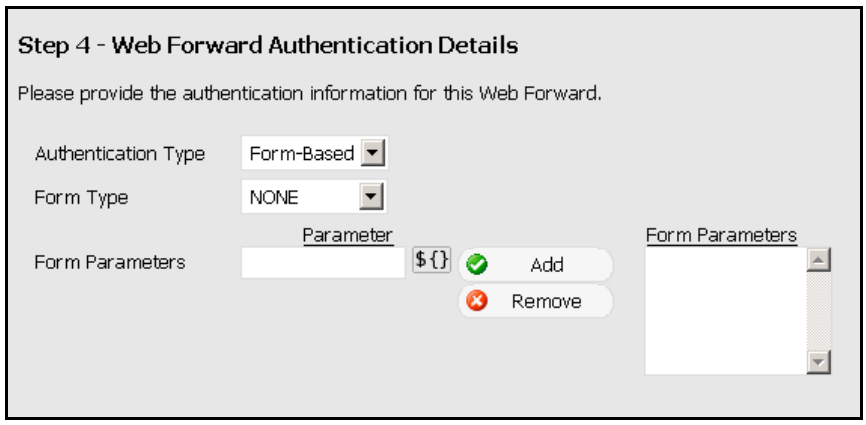
The second part of information required is the authentication details.

Authentication

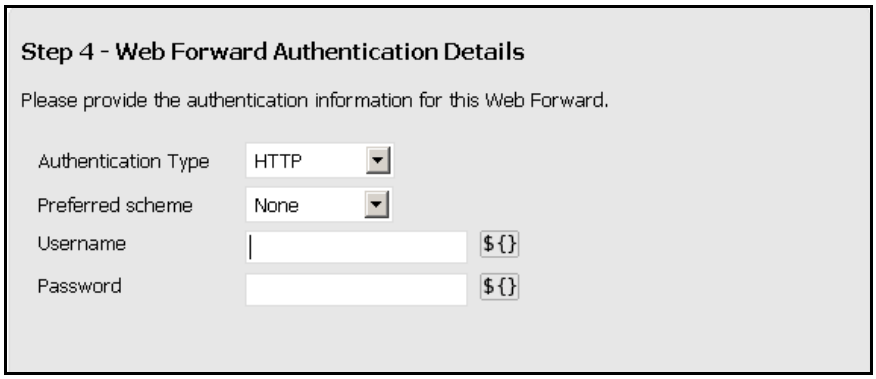
Replacements and reverse proxy can not only access a site or an application but can also authenticate the user accessing it. When the Web forward connects to the URL the additional information provided here are passed in to the site automatically authenticating the user.

Depending on the type of authentication type you select in the dropdown the appropriate parameters are listed.

The wizard provides two types of authentication FORM and HTML authentication.



- **Form Type:** The type of form authentication to use, in most circumstances POST will be used to post the parameters listed in the Form Parameters box to the site. NONE disables form authentication and relies on HTML authentication only.
- **Form Parameter:** Specific form parameters for authentication should be provided here. These parameters map to the parameters on the form. As the example above `pre, ixPerson, sPassword` are all form parameters for this application. During authentication these will be passed into the form with the provided values. As `sPassword=${session:password}` shows replacement parameters can also be used, we have used a session parameter for the form's password field. The `ixPerson` parameter is the index list for forms username dropdown list, 6 is the index of the given username, when executed the form will lookup username 6 from the dropdown list.



- **Preferred scheme:** The type of HTML authentication to be used, BASIC, NTLM, DIGEST, NONE.
- **Username:** The authenticating username for HTML authentication, each scheme uses this value in different ways.
- **Password:** The associated password.

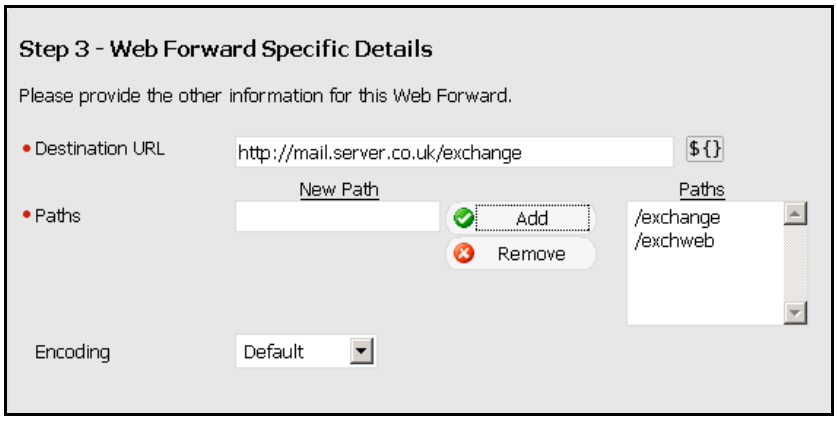
Depending on the site whichever authentication method is required by the server those details will be passed forward.

Once completed pressing the **Next** button will proceed to the next step in the wizard, this is detailed in step 6 below.

Configuring a Reverse Proxy Web Forward

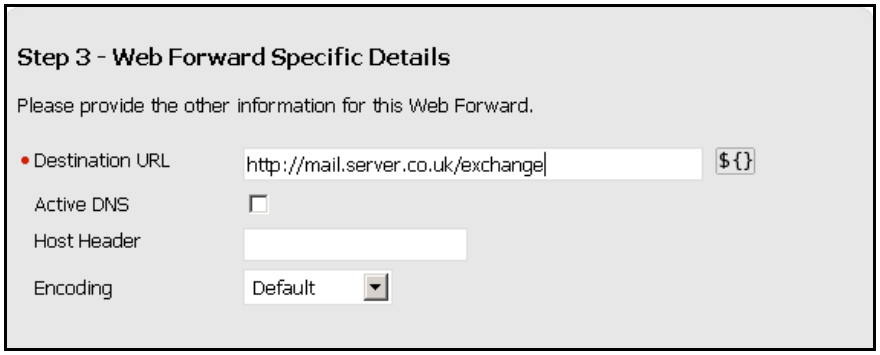
As with replacement proxy this also requires two types of information, the basic URL information and the authentication details however unlike other Web forwards this is broken into host-based proxy and host-based proxy.

The Path-Based Reverse Proxy Method



- **Destination URL:** The URL of the site you wish to access
- **Paths:** Each additional path that needs to be proxied is added here. Web applications such as Outlook Web Access require more paths than the one in the target URL, in the example above the OWA Web forward sets a target of `http://mail.server.co.uk/exchange` and then adds 2 further paths `/exchange`, `/exchweb`. To deal with this, you add each path that should be proxied to this filed. This would then proxy any URLs that begin with `http://mail.server.co.uk/exchange`, and `http://mail.server.co.uk/exchweb`
- **Encoding:** This overrides the encoding of the HTTP response; this should be left as default unless otherwise informed a Barracuda Central engineer.

The Host-based Reverse Proxy Method



- **Active DNS:** This enables sites that are at root of a server to be used by the Web forward, as mentioned in the note above sites at root generally cannot be used by the reverse proxy Web forward. Enabling this parameter is not enough, a wild card entry on your networks DNS server must be configured so that any lookups for active `*.example.com` point to the Barracuda SSL VPN. When the Web forward is launched a fake hostname prefixed by active

and suffixed by `example.com` is generated (e.g. `active32432432424.example.com`) and used by the client browser to access the reverse proxy. The Barracuda SSL VPN is able to see this hostname and use the number embedded to look up the associated Web forward.

- **Host Header:** This is another method used by the reverse proxy engine to determine whether a site should be proxied. A specific hostname can be set for a site this requires that the hostname defined resolves to the Barracuda SSL VPN. The browser will be redirected from the standard URI to this host header.

No Target Site at Root of Server
Ordinarily target sites you wish to use with reverse proxy cannot exist at the root of their server. e.g. `http://www.example.com` is invalid whereas `http://www.example.com/salesportal` would be acceptable. Active DNS can be used to override this action.

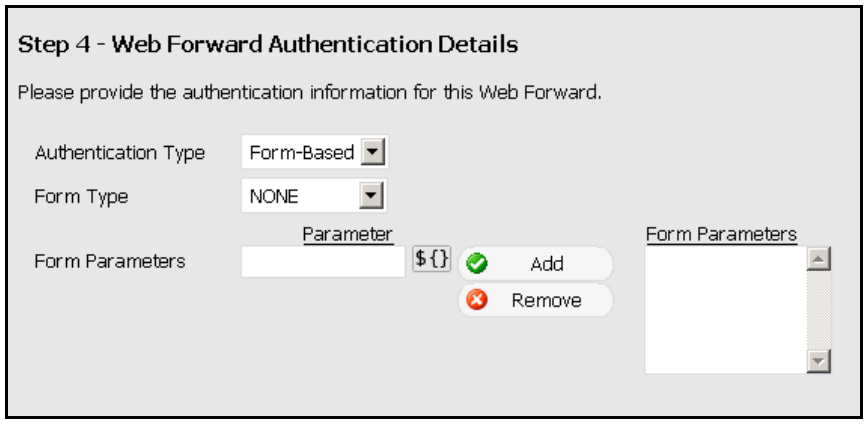
The second part of information required is the authentication details.

Authentication

Replacements and reverse proxy can not only access a site or an application but can also authenticate the user accessing it. When the Web forward connects to the URL the additional information provided here are passed in to the site automatically authenticating the user.

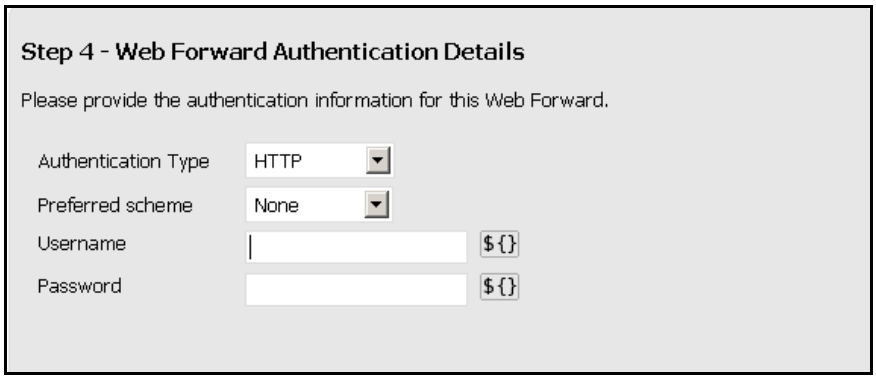
Depending on the type of authentication type you select in the dropdown the appropriate parameters are listed.

The wizard provides two types of authentication FORM and HTML authentication.



- **Form Type:** The type of form authentication to use, in most circumstances POST will be used to post the parameters listed in the Form Parameters box to the site. NONE disables form authentication and relies on HTML authentication only.
- **Form Parameter:** Specific form parameters for authentication should be provided here. These parameters map to the parameters on the form. As the example above `pre,`

`ixPerson, sPassword` are all form parameters for this application. During authentication these will be passed into the form with the provided values. As `sPassword=${session:password}` shows replacement parameters can also be used, we have used a session parameter for the form's password field. The `ixPerson` parameter is the index list for forms username dropdown list, 6 is the index of the given username, when executed the form will lookup username 6 from the dropdown list.



- **Preferred scheme:** The type of HTML authentication to be used, BASIC, NTLM, DIGEST, NONE.
- **Username:** The authenticating username for HTML authentication, each scheme uses this value in different ways.
- **Password:** The associated password.

Depending on the site whichever authentication method is required by the server those details will be passed forward.

Once completed pressing the **Next** button will proceed to the next step in the wizard.

Step 5 Once the Web forward has been successfully configured the next step is the assignment of the resource to a policy. The appropriate policy should be added to Selected Policies box.

Step 6 In the final step the wizard presents a summary of the Web forward. Pressing the Finish button will end the wizard and create the Web forward. This newly created Web forward will be visible from the main Web forwards page and executable by those in the assigned policy.

Editing a Web Forward

From the Web forwards page select the **Edit** action against the required Web forward and the Edit Web Forward page will be shown. From this page the current details stored about the Web forward can be modified.

Deleting a Web Forward

The **Delete** action removes a Web forward permanently from the system. Selecting the delete action against a Web forward will result in a warning message informing that the Web forward is about to be deleted, as shown below.

Selecting **Yes** will result in the removal of the resource from the system. If this Web forward is associated with any policies this link will also be removed along with all other associated links.

Outlook Web Access and Mail Check

This mail check feature presents to the user an instant view of his or her email account status directly through the user console without having to start their email client to check for new email. This feature can be used to check for email (and launch your Web mail client) on any mail server that supports the POP3/IMAP protocols, including Microsoft Exchange.

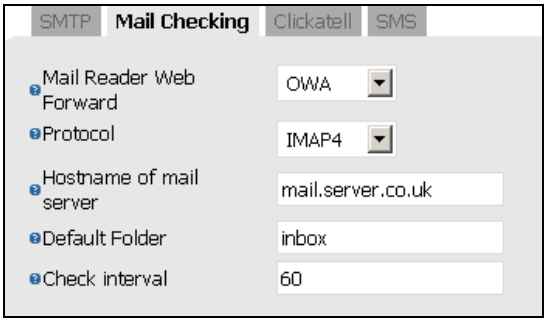
The mailbox icon is visible from the user console and shows the status of new or any unread messages.

Clicking the refresh button also instantly checks the mail account and provides an instant update of its status and clicking the mailbox itself will open a new window to the mail account.

Configuration of this relies on a Web forward. The following provides basic steps on how to configure the mail check feature.

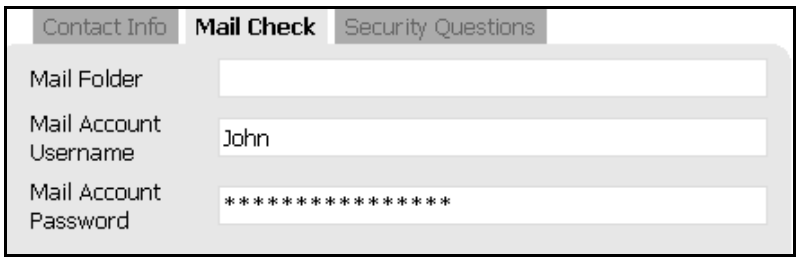
Step 1 Create a Web forward that connects to the mail server and check that it works correctly. In the screenshot below we have created an Outlook Web Access (OWA) Web forward. No username or password has been specified in the configuration. When this Web forward is launched we will be prompted for authentication.

Step 2 Configure the mail check configuration parameters from **Management Console** > **Configuration** > **Messaging** > **Mail Check**.



The mail check feature requires the OWA server's details to access the mail server. Also the mail protocol has been specified and the hostname of the mail server.

Step 3 The final step involves the configuration of personal details for each user from the user console. For each user the mail check tab becomes accessible from **User Console** > **Personal Details** > **Mail Check**.



The Mail Check extension will automatically try and log onto the mail server with the currently logged on users credentials. When using Active Directory authentication along with a Microsoft Exchange

mail server these are usually identical. If these are different, then each user needs to provide their mail authentication details on this screen. In addition the default mail folder (e.g. 'inbox') can be specified if needed.

Active Directory Accounts Auto Configured
If the system has been configured to use Active Directory and the mail accounts also uses the same Active Directory authentication credentials, the mail check extension will automatically use the user's Active Directory credentials to authenticate the user's mail account. There is then no need for users to provide authentication details in the mail check tab under personal details.

The mail check feature uses the Web forward and the details defined in the mail check configuration page to connect to the mail server. It is from here it takes the individual users authentication details to connect to their account and retrieve mail details.

Step 4 Once all the user details have been provided the user should log back into the system. The mailbox icon will be visible in the top right of the main window.

Clicking on the mailbox will open a window to the mail account of the user without the need for authentication.

Network Places

Network places are another vital tool against defending unwarranted access to the corporate network. By configuring a network place in the Barracuda SSL VPN, this allows a user to securely access the company network without compromising the integrity of the network. This chapter covers the basics of network places and moves right through to managing these resources.

By the end of this chapter the reader should have a firm grasp on network places and how best to use them in particular the means in which a simple network forward can be integrated into a user's familiar Microsoft Windows environment.

What is a Network Place?

A network place is a versatile resource that provides remote users with a secure Web interface to the corporate network. A remote user can browse network shares, rename, delete, retrieve and even upload files just as if he or she was connected in the office connected to the network.

In particular network places provide remote users that have appropriate permissions to browse Microsoft Windows file shares, SAMBA file systems configured on UNIX and even FTP or SFTP file systems. In addition network places also provide support for Web folders and the Windows Explorer Drive Mapping feature.

Web Folders

Web Folders is a Web authoring component that is included with Internet Explorer 5. It enables the management of files on a WebDAV server by using a familiar Windows Explorer interface.

WebDAV is a protocol that extends HTTP to define how basic file functions such as copy, move, delete, and create folder are performed over the internet. Using a WebDAV client as Web folders a remote user can access the company network through the standard Windows Explorer interface without actually needing to log into the Barracuda SSL VPN.

Network Places Interface

The main network place page lists the available shares. This page is located under **Management Console** > **Resources** > **Network Places**

The main page details which policy a network place is associated with and the available actions associated with each.

Only those network places associated with a user's policy are visible from the user console under **User Console** > **Resources** > **Network Places**.

Action Icons

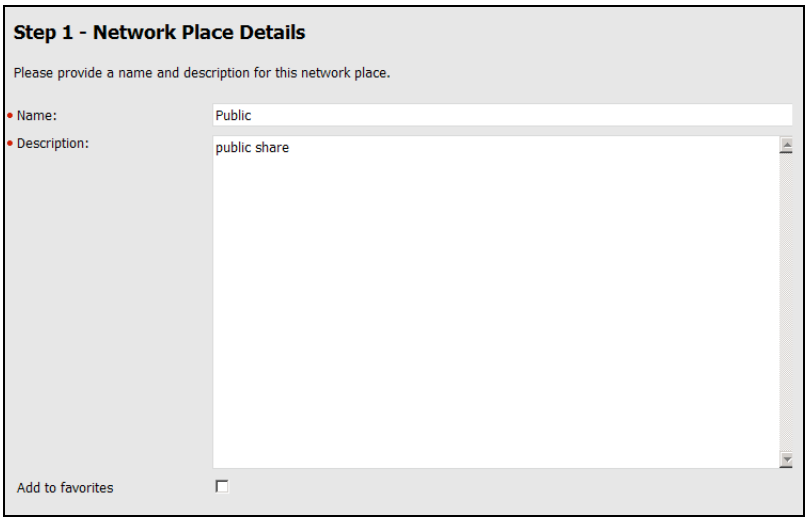
The action icons against each network place performs functions on the associated network place, their respective objective are detailed below:

	Delete network place
	Edit network place details
	Execute resource (user console)

Creating a new Network Place

Step 1 From the main network places page the action menu in the top right presents the only available action which is, Create Network Place. Selecting this begins the creation wizard.

Step 2 The first step in the wizard as with any resource is the name and the description of the required resource. This will be displayed on the main network places page.



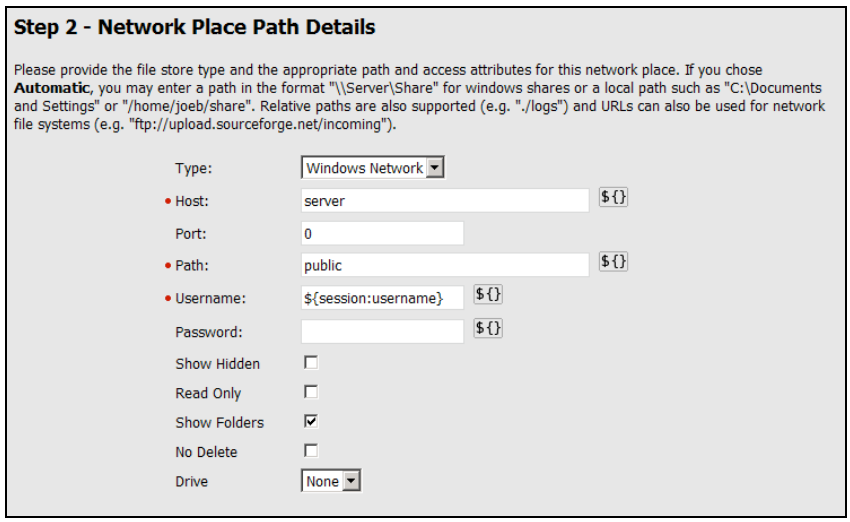
This particular resource can be added to the favorite page if so desired for ease of access.

Step 3 The next step requires the definition of the URL alongside any additional parameters. Selecting the Type

This can be of the following:

- **Windows Network:** Windows source anywhere on a visible network
- **FTP:** FTP filesystem
- **SFTP:** SFTP filesystem
    - **Automatic:** This allows the user to type in single URLs for any type of filesystem and it will try to determine the correct type of system.

Step 4 Depending on the type chosen a list of parameters are shown and need completing.


Step 2 - Network Place Path Details
Please provide the file store type and the appropriate path and access attributes for this network place. If you chose Automatic, you may enter a path in the format "\\Server\Share" for windows shares or a local path such as "C:\Documents and Settings" or "/home/joeb/share". Relative paths are also supported (e.g. "./logs") and URLs can also be used for network file systems (e.g. "ftp://upload.sourceforge.net/incoming").
Type:
Windows Network
Host:
server
Port:
0
Path:
public
Username:
${session:username}
Password:
Show Hidden
Read Only
Show Folders
No Delete
Drive
None

- **Host:** Hostname of source filesystem
- **Port:** Port of source filesystem
- **Path:** Specific path that needs to be accessed on the host

Note

Replacement Variables

The `${}` indicates that replacement variables can be included in the resource definition. Click this icon will load the available variables that can be used. The `session` variables are values taken from the current session. The `args` variables are values taken from user defined attributes.

- **Username:** Username if the location is protected. If this is to be used by all users then the replacement variables should be used such as ${session:username}
- **Password:** Password for the username

Note

FTP Default Passive

FTP can initiate connections in passive and active mode. By default all ftp URI's will be connected to their host using passive mode as this is the most secure and most common mode used. However if you wish to connect to a server in non-passive mode simply add `?passive=FALSE` to the end of the URI as in `ftp://ftp.server.com?passive=FALSE`.

Step 5 In addition to defining the path a network place resource requires its access permissions defining. This will restrict what access rights will be available on the file share when a user executes the network place. The available permissions are as follows:

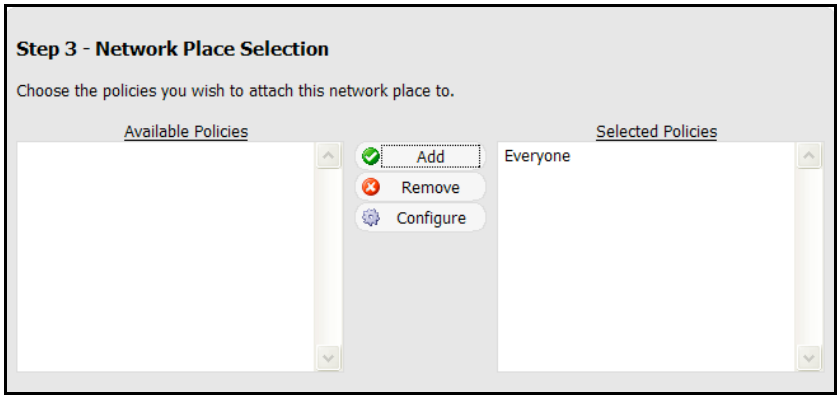
- **Show hidden:** Show all files and folders including hidden files
- **Read Only:** All files folders are visible but they can only be viewed
- **Show Folders:** Show only folders
- **No Delete:** All files and folders are visible and all file management actions can be performed except deletion of any files

A combination of these can be chosen.

The final step is defining a drive letter for the network place. This feature allows a share to be mapped to a drive letter. Once mapped the user is able to access the network share through Windows Explorer no longer needing to connect to the Barracuda SSL VPN to see the content.

- **Drive:** Select a drive to map to this network place. Refer to the section titled Windows Explorer Drive Mapping

Step 6 Once the network place has been defined the final step is in the defining which policy this network place should be associated with. Any user not linked to this policy will not be able to access the network place.



Step 7 The wizard provides a summary of the wizard, pressing Finish completes the process and creates the new resource.

The newly created network place will be visible from the main network place page.

File Management

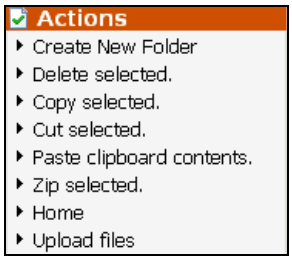
When a network place is executed the file system is opened in a new window. The window displays the content of the file. All the content from here and below can be managed; files removed, uploaded and even deleted as if you were connected directly to the file system.

Depending on what permissions were selected during the configuration of the resource depends on what actions are available to the user.

The full list of available actions against each file is listed below.

	Delete selected file or folder
	Rename selected file or folder
	Copy selected file or folders
	Cut selected file or folder
	Paste content of clipboard to selected folder
	Zip folder and store it to a locally accessible file system

In addition to these action icons the actions available in the Actions pane in the top right of the window also perform these functions as well as the ability to **Upload** files and return back to the top folder (**Home**).



Editing a Network Place

From the network place page select the **Edit** action against the required resource and the Edit Web Forward page will be shown. From this page the current details stored can be modified.

Deleting a Network Place

The **Delete** action removes a network place resource permanently from the system. Selecting the delete action against a network place will result in a warning message informing that the resource is about to be deleted, as shown below.

Selecting **Yes** will result in the removal of the resource from the system. If this network place is associated with any policies this link will also be removed along with all other associated links.

Web Folders Windows Access

When using Windows XP or later along with Internet Explorer, you can take advantage of Microsoft Web Folders to access your file resources.

Web folders are a great tool for remote working and once set up accessing a share is simply a matter of clicking an icon and entering a Windows username and password when prompted.

So any Web folder configured must go through the Barracuda SSL VPN server else the share cannot be seen by the client operating system.

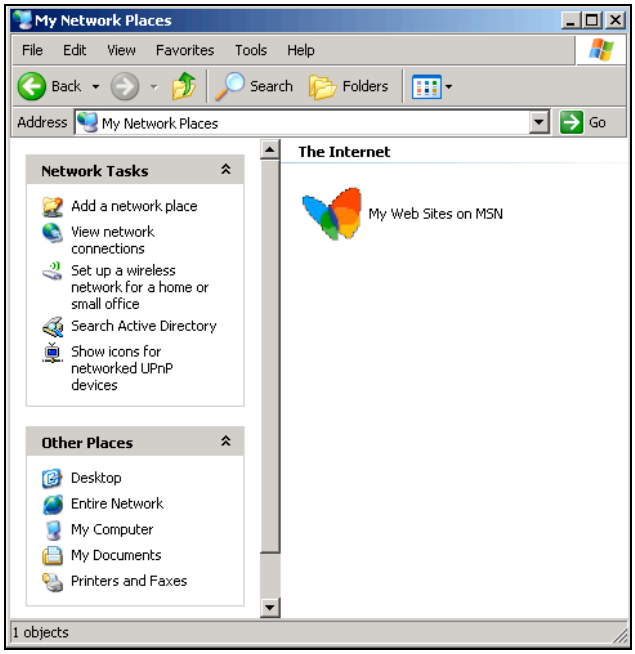
For security the Barracuda SSL VPN only allows Web folders to be mapped to existing network places. If a network file system has not been configured through network places then the Web folder cannot be mapped to the desired location. This enforces the policy restrictions; if a user does not have a policy which allows them to access a given network place then they can neither create a Web folder to it.

The steps to create a Web folder are listed below.

Step 1 The required file system should already exist as a network place.

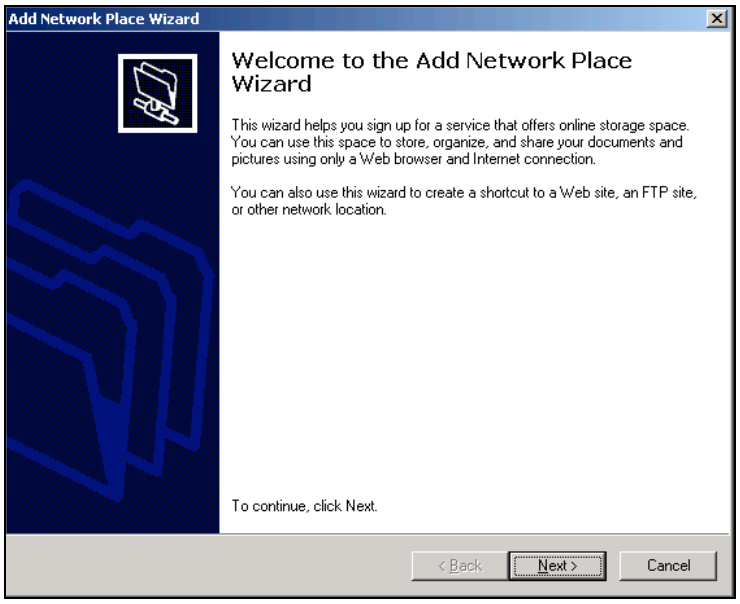
The network place should be configured to access the appropriate share. It is the name used here that will be used to look up the configured URI.

Step 2 From Windows access **My Network Places**.

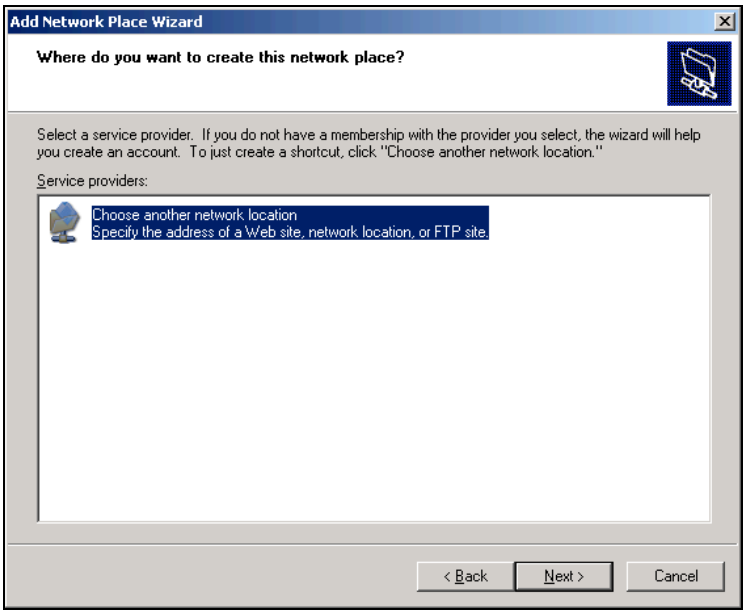


Step 3 Under the Network Tasks pane select **Add a network place**.

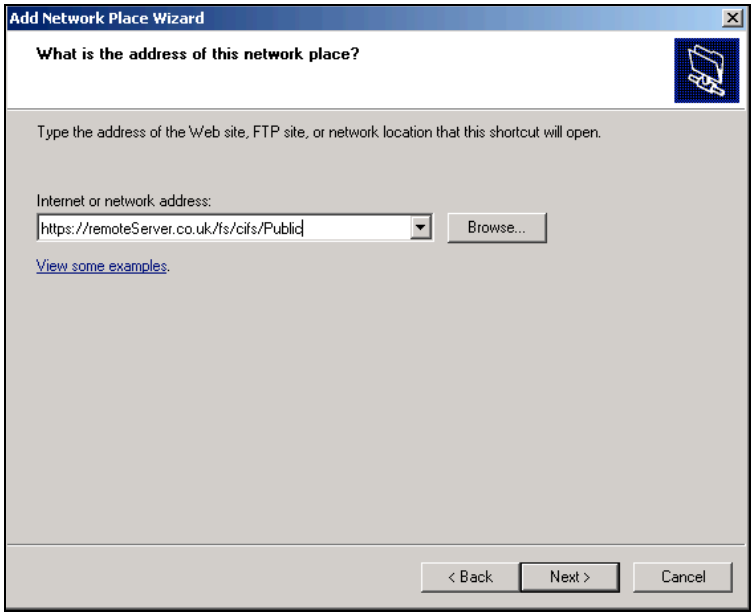
Step 4 This starts the Add network place wizard.


Add Network Place Wizard
Welcome to the Add Network Place Wizard
This wizard helps you sign up for a service that offers online storage space. You can use this space to store, organize, and share your documents and pictures using only a Web browser and Internet connection.
You can also use this wizard to create a shortcut to a Web site, an FTP site, or other network location.
To continue, click Next.
< Back
Next >
Cancel

Step 5 The wizard will briefly search for information about service providers and will then present you with the following screen. Select **Choose another network location** and click next.


Add Network Place Wizard
Where do you want to create this network place?
Select a service provider. If you do not have a membership with the provider you select, the wizard will help you create an account. To just create a shortcut, click "Choose another network location."
Service providers:
Choose another network location
Specify the address of a Web site, network location, or FTP site.
< Back
Next >
Cancel

Step 6 Now you need to enter the fully qualified domain name to your Barracuda SSL VPN server.

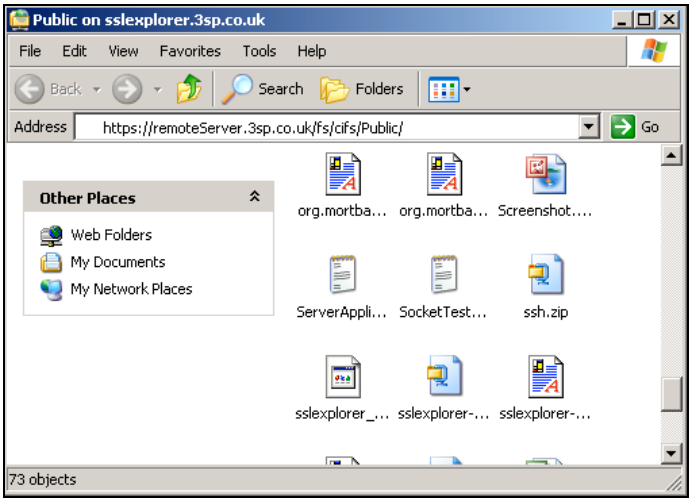

Add Network Place Wizard
What is the address of this network place?
Type the address of the Web site, FTP site, or network location that this shortcut will open.
Internet or network address:
https://remoteServer.co.uk/fs/cifs/Public
Browse...
View some examples.
< Back
Next >
Cancel

In the screenshot above the Barracuda SSL VPN is `https://remoteServer.co.uk` and my network place as named in network places on the system is `Public`.

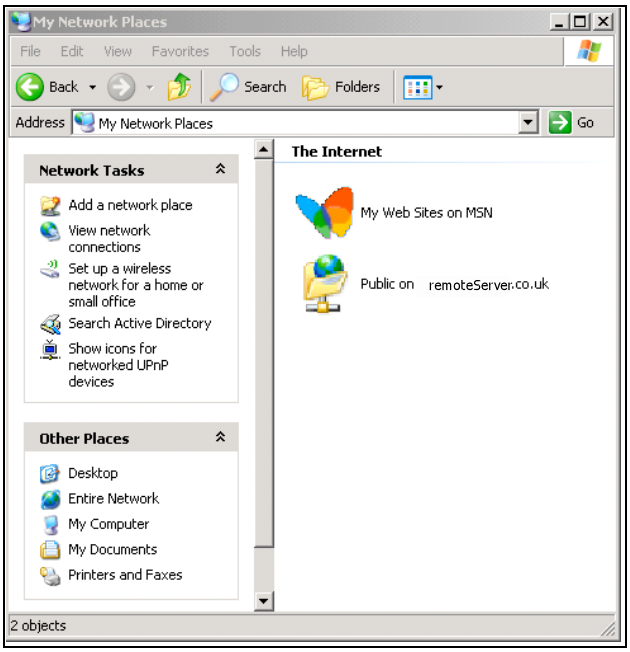
When executed Web folders will locate communicate with the appliance at `remoteServer.co.uk`. It will then request the URI for a network place named `Public`. It is this URI that will then be mapped to the Web folder.

Step 7 The Web folders client will attempt to connect to the resource and you will be prompted to enter your authentication details.

Step 8 After successful authentication the client will ask for a new name for this network place. Windows has successfully created the Web folder. Windows Explorer opens and searches for resources. You may be asked to accept a certificate as part of the process – this is normal and ensures that your data is encrypted across the wire using SSL.



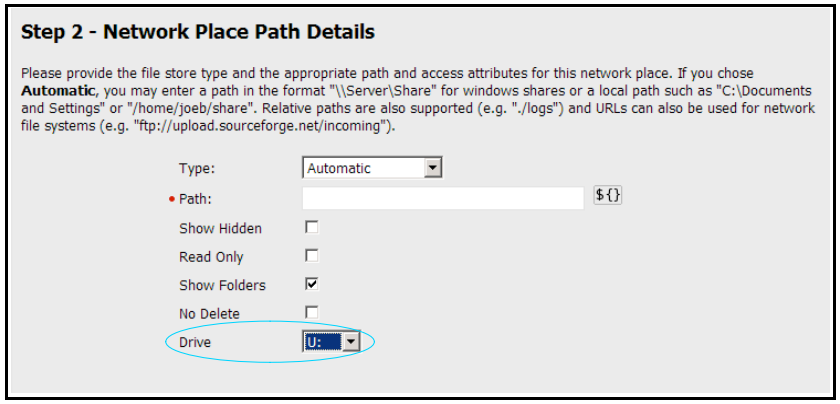
In 'My Network Places' a new shortcut is created.



This shortcut can be moved to the desktop so that all a user needs to do to access the shared folder is double-click this icon and enter your Windows logon information.

Windows Explorer Drive Mapping

This feature adds the ability for a user to create a network place and assign it a drive letter when using Microsoft Windows 2000 or later.


Step 2 - Network Place Path Details
Please provide the file store type and the appropriate path and access attributes for this network place. If you chose Automatic, you may enter a path in the format "\\Server\Share" for windows shares or a local path such as "C:\Documents and Settings" or "/home/joeb/share". Relative paths are also supported (e.g. "./logs") and URLs can also be used for network file systems (e.g. "ftp://upload.sourceforge.net/incoming").
Type:
Automatic
Path:
${}
Show Hidden
Read Only
Show Folders
No Delete
Drive
U:

The effect of this is that once the Barracuda SSL VPN Agent is running the drive becomes available under the user's Windows Explorer and like any other drive listed in Windows Explorer this drive can be accessed and any content accessible for the lifetime of the Agent.

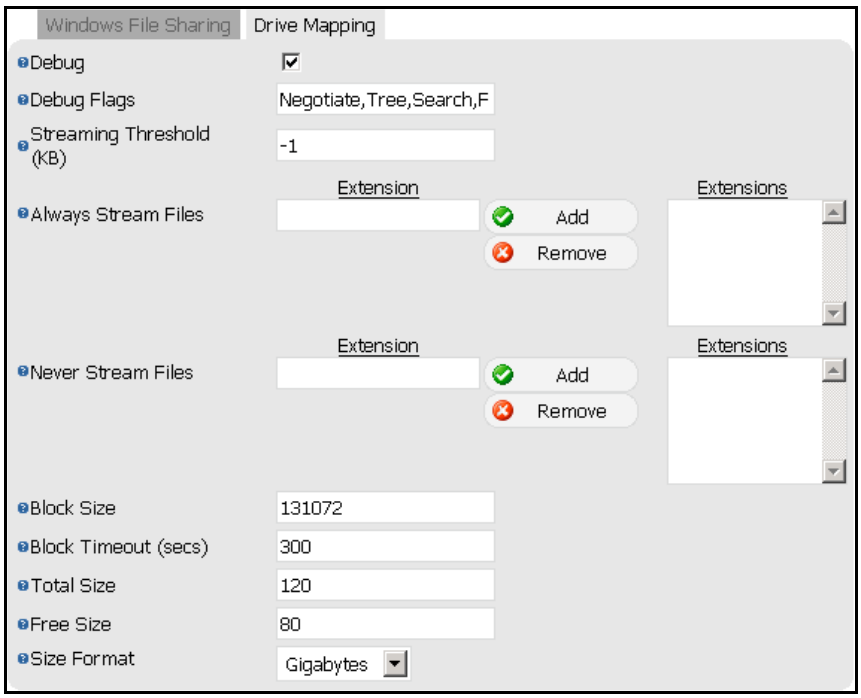
How does this differ from WebDAV?

WebDAV is limited to what file types it can support, certain files require specific WebDAV support added to them in order to be accessed while others are not accessible at all. With the drive mapping feature, any file can be accessed, modified and saved as long as it supports random access can be accessed and are fully modifiable.

Not only that but WebDAV supports only local buffering, any file needing to be edited WebDAV will download a local copy and it is this copy that is edited. Once editing is complete WebDAV uploads this back to the server. With the drive mapping feature any file can be edited in the traditional local buffered mode or also via streaming mode where the file is edited directly from the source.

Configuring Windows Explorer Drive Mapping

A number of configuration properties can be accessed from **Management Console** > **System Configuration** > **Windows Integration** > **Drive Mapping** and are detailed below.



- **Debug:** Enable debugging for drive mappings. This should only be set if asked by a Barracuda Central engineer.
- **Debug Flags:** Flags for the above debug option.
- **Streaming Threshold:** The size at which files are streamed. Streaming maintains an open file on the remote filesystem. A zero value means files are always streamed.
- **Always Stream Files:** The file extensions that should always be streamed.
- **Never Stream Files:** The file extensions that should never be streamed.
- **Block Size:** The block size used when reading data from the remote file system. Altering this value can affect the efficiency of file access and the default value should be ample for most environments.
- **Block Timeout:** The number of seconds before a timeout exception is thrown when reading streamed blocks of data from the remote file system. A timeout exception will cause unexpected results and as such this setting is only used when the remote file system becomes unresponsive. It is not recommended that you change this value unless instructed to do so by a Barracuda Central engineer.
- **Total Size:** The total amount of disk space displayed for a drive's volume information
- **Free Size:** The amount of free space displayed for a drive's volume information
- **Size Format:** The format to use in a drive's volume information

Applications

This feature of the Barracuda SSL VPN allows for the publishing of applications that are to be either downloaded or launched by your clients. The benefits of being able to distribute resources in this way are mainly linked with convenience and reduced costs of distributing applications and dependant software.

This section will cover:

- What is an Application Shortcut?
- Applications Interface
- Publish a new Application
- Edit an Existing Application
- Removing an Application

What is an Application Shortcut?

An application shortcut allows for the publication of an application via the Barracuda SSL VPN appliance. This means an application can be distributed very easily to authorized clients. This prevents the need to install specific application software on each client. In order for an application shortcut to function it requires the following information:

- Shortcut Identity
- A valid Extension type
- A valid Application shortcut configuration
- Associated Policy

The other major component to an application is the extension that is associated to it. The extension is in essence the method of connection to be used to gain access to the application

Applications Interface

The main applications page provides information on all applications present within the system. By hovering over any resource a pop-up is loaded that provides information on the details of each resource, in this instance the key information is detailed below:

- **Name:** The name of the Application shortcut.
- **Type:** The Extension type.
- **Description:** Further details on the resource

Action Icons

The action icons against each application shortcut performs functions on the associated application shortcut, their respective objective is detailed below:

	Delete Application shortcut
	Edit Application shortcut details
	Execute resource (user console)

Publish a new Application

In order to demonstrate the publishing of a new application this section will detail the steps required to use the UltraVNC Extension to create a VNC connection to a system.

UltraVNC is easy to use, fast and free software that can display the screen of another computer (via internet or network) on your own screen. The program allows you to use your mouse and keyboard to control the other PC remotely.

License: It is free and open source software released under the GNU General Public License.
Official Site: http://www.ultravnc.com/

Step 1 First browse to **Management Console** > **Resources** > **Applications**.

Step 2 In order to publish a new application, click the Create Application Shortcut in the action menu.

This starts the Create Application Wizard.

Step 3 In this screen the type of application extension is defined. The wizard behavior changes for step three. This is due to each application type having potentially different requirements for operating information. UltraVNC is used in this example but the other application types are covered later in this section. Select **Next**.

The next screen allows for the entry of the application details. A brief description of each of the fields follows.

- **Name:** The name to be used to identify the application shortcut.
- **Description:** A description of the application shortcut.
- **Add to favorites:** A checkbox that if selected will add the application shortcut to the favorites of the appropriate accounts.

Step 4 When the fields have had the desired values entered simply click the **Next** button.

As already mentioned, depending on the application type a different Application Options screen will be presented. In this instance UltraVNC is being used. Each of the options available on the different tabs is explained below.

General Tab

Each of the options is described briefly below:

- **Hostname:** Hostname of the remote VNC server that is being connected to.

- **Port:** The port on which the remote is listening. If the VNC server uses display numbers instead of ports (i.e. if the VNC server is hosted on a Linux system), simply add 5900 to the display number to get the port number.
- **Password:** The password for the remote VNC server.

Display Tab

Each of the options is described briefly below:

- **Full Screen:** When enabled the remote desktop session will take up the entire screen.
- **Display Scale:** Magnify or reduce the display area of the remote desktop.
- **Disable Status Bar:** Disables the Status Bar when connecting to a WinVNC server.
- **Disable Hot Keys:** Disables the WinVNC Hot keys.
- **Disable Toolbar:** Disables the UltraVNC Toolbar.
- **View Only:** Local mouse and keyboard input is disabled.
- **Cursor Type:** Displays a specific type of cursor in the display window.
    - **No Cursors:** Local systems current cursor type.
    - **Dot Cursor:** A small dot as the remote cursor.
    - **Normal Cursor:** Displays the remote cursor.

Mouse Tab

Each of the options is described briefly below:

- **Emulate 3 button mouse (2 button click):** Pressing the left and right mouse button at the same time emulates a middle mouse button click (i.e. LMB + RMB = MMB).
- **Swap Mouse Buttons:** Swaps the functions of the left and right mouse buttons.

Protocol Tab

Each of the options is described briefly below:

- **Colour Scheme:** Alters the color scheme of the display.
- **Share the Server with other viewers:** Allows other VNC viewers to connect, view and control the remote desktop.
- **Compression Level:** The level of compression to be used when supported by a particular form of encoding. The lower the number the less compressed which has a saving against processor time.
- **Do not transfer Clipboard contents:** This prevents the contents of the clipboard from being transferred to the remote client/viewer.
- **Encoding:** Allows the selection of encoding types for the session.

Advanced Tab

Each of the options is described briefly below:

- **Level of Logging:** Change level of log output. Use higher numbers to aid debugging.
- **Output Console:** Display log output on the console.

Once the application options have been entered click the next button to advance to the next page.

Step 5 This page allows for the configuration of policies to be applied against the new application record. Policies can be added, removed or even configured from his page. When all relevant policies have been applied click the **Next** button which displays the summary page.

Step 6 If all information on this page is correct press the **Finish** button to advance to the final wizard page.

Step 7 Clicking the **Exit Wizard** button returns to the main applications page where the newly created applications record is present.

This shortcut can now be executed and the configured resource will connect to the remote machine.

Edit an Existing Application

Step 1 To edit an existing application navigate to the applications screen (**Management Console** > **Resources** > **Applications**). A list of existing applications is displayed as shown below.

Step 2 To edit an application just click the **Edit** action against the application to be altered.

This will then show a tabbed screen where values can be changed for all of the associated information against an application. In the following example an UltraVNC application type is shown.

Step 3 Clicking the **Save** button will store the altered values and redisplay the applications screen. Selecting the **Cancel** button will not alter any values and return to the application screen.

Removing an Application

Step 1 To remove an existing application, navigate to the applications screen (**Management Console** > **Resources** > **Applications**). A list of existing applications is displayed.

Step 2 To remove an application, select the **Remove** action against the application to be removed.

The following screen is presented.

Step 3 Selecting **No** will cancel the action and return to the application screen. Selecting **Yes** will remove the application and return to the main application screen.

SSL Tunnels

SSL Tunnels allow for ad-hoc connections to be made between networked computers.

What is an SSL Tunnel?

An SSL Tunnel is simply a connection between two TCP enabled components. All of the data transmitted over a tunnel is encrypted using the SSL protocol. This is done the same way as other tunneling technologies.

For example, a user may wish to create a secure tunnel to a TCP/IP enabled database. First of all, an administrator configures a new SSL tunnel that uses 63389 as its source port and `example.company.dom:3389` as the destination. The user may then activate this tunnel and then specify `localhost` as the hostname and the 63389 as the port and all traffic with then be secured.

You may use the same technique for a number of different applications and protocols. A common use of tunnels is to secure the SMTP / POP protocols used for email access. In short, anything that uses TCP/IP client / server architecture will usually be able to be secured in this manner.

Tunnel Types

Tunnels come in two types:

- **Local:** A local forwarding is where the client acts as the listening device.
- **Remote:** A remote forward is where the client acts as the listening process. Here the roles are reversed and it is the remote target that acts as the listener of any communication request. The practical implication of this is that a remote user can connect to a central company networked SSH server and use it as a go between to access another client machine within that network.

SSL Tunnels Interface

The SSL tunnels page is accessible from **Management Console → Resources → SSL Tunnels**.
The main SSL tunnels page provides information on all tunnels present within the system.

Action Icons

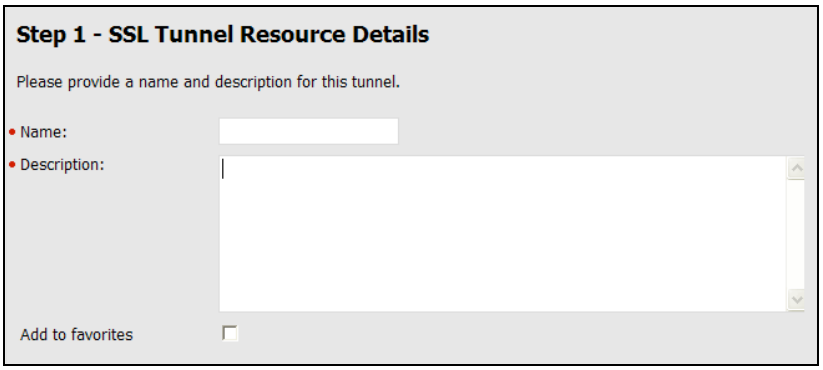
The action icons against each SSL tunnel performs functions on the associated tunnel, their respective objective is detailed below:

	Delete SSL Tunnel
	Edit SSL Tunnel details
	Execute resource (User Console)

Create a new SSL Tunnel

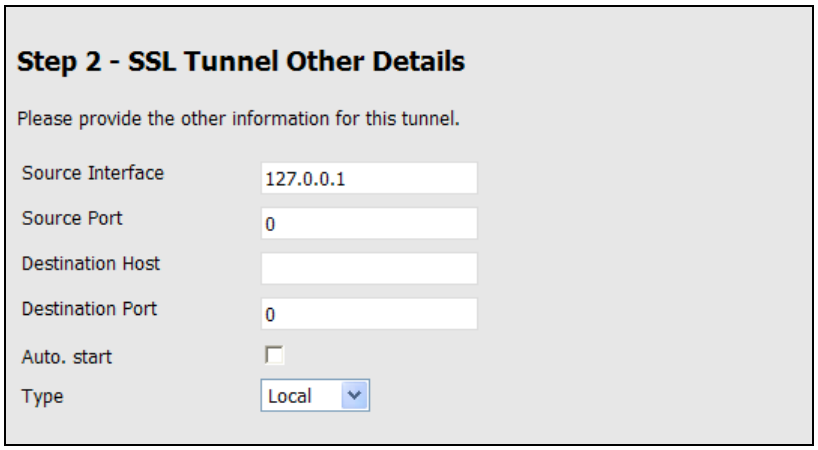
Step 1 To create a new SSL tunnel, first click the "Create Tunnel" action from the SSL tunnel main page.

This will then start the wizard, the first page of which follows.


Step 1 - SSL Tunnel Resource Details
Please provide a name and description for this tunnel.
Name:
Description:
Add to favorites

- **Name:** The name to be used to identify the SSL tunnel.
- **Description:** A description of the SSL tunnel.
- **Add to favorites:** A checkbox that if selected will add the SSL tunnel to the favorites of the appropriate accounts.

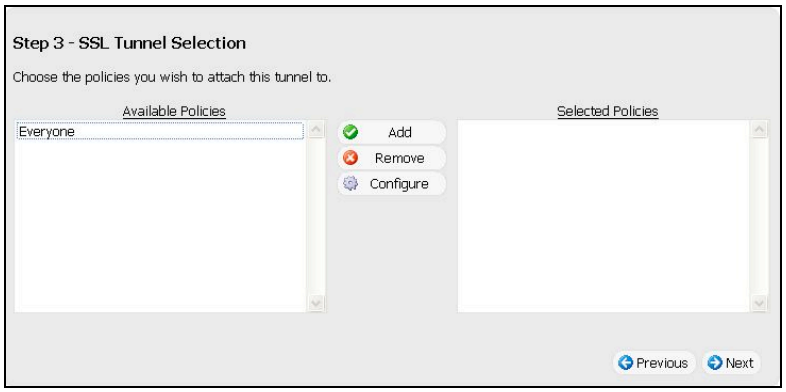
Step 2 Once all the relevant values have been completed simply click the Next button. This will show the following page.



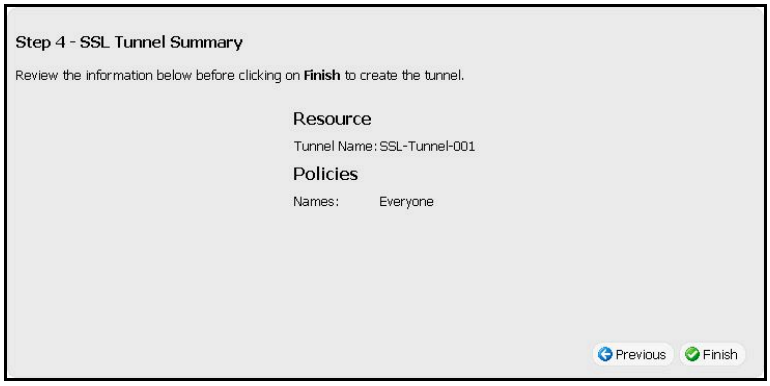
- **Source Interface:** The interface the local server will listen on. This can be any valid local IP address. For example, it could be your network IP address in which case you would connect to <hostname>.com in this case other external hosts will be able to connect to you via your hostname. This replaces the original allow external hosts parameter. It could also be 127.0.0.1 in which case the local loopback address localhost will be used. In this case only you can connect using localhost or 127.0.0.1. It could also be blank in which case it will listen on both.
- **Source Port:** The port number to use with the source interface. The port on which the client Agent creates a server that is connected via the tunnel to the destination on the network. This can be any port number (over 1024 on UNIX based systems) and is the number that should be used when configuring the client application. For example, if you were connecting a tunnel from port 60025 to an SMTP server running on port 25 on the host mail.mycompany.com, the source port is 60025.
- **Destination Host:** The name of the host that forms the other end of the tunnel.

- **Destination Port:** The port number of the host that forms the other end of the tunnel. The port on which the Barracuda SSL VPN creates a server that is connected via the tunnel to the Agent which then is in turned connected to the client application (a server of some kind, VNC server for example – in this case people on the appliance would be able to use a VNC viewer to display and control the remote desktop e.g. this would run on port 5900).
- **Auto. Start:** A checkbox that is disabled as default. When checked this will automatically try to start the tunnel for the duration of the session.
- **Type:** This drop down box supports the values Local and Remote. A local SSL tunnel type allows for local connections only. The Remote option will allow for connections to the remote clients network.

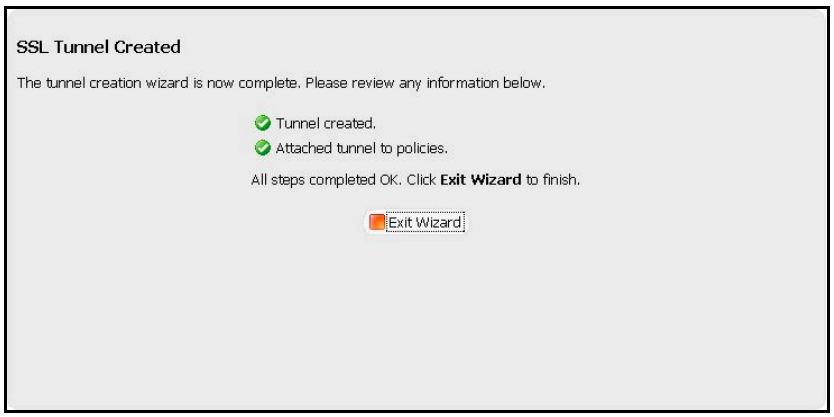
Step 3 Once all the relevant values have been completed simply click the **Next** button. This will show the following page.



Step 4 Once all the relevant values have been completed simply click the **Next** button. This will show the summary page.



Step 5 If the summary information is all correct simply click the **Finish** button. This will show the final wizard page.


SSL Tunnel Created
The tunnel creation wizard is now complete. Please review any information below.
Tunnel created.
Attached tunnel to policies.
All steps completed OK. Click Exit Wizard to finish.
Exit Wizard

Step 6 Finally click on the **Exit Wizard** button to close and exit the wizard. The newly created SSL tunnel will now be displayed on the main page.

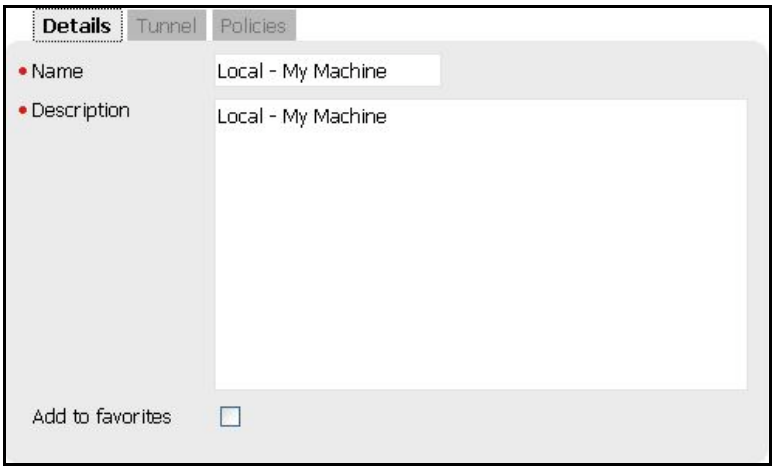
In addition to this a new item will become available from the User Console as shown below (Navigation is: **User Console → Resources → SSL Tunnels**). SSL tunnels require the Barracuda SSL VPN Agent to be running in order to operate correctly.

Edit an existing SSL Tunnel

Step 1 To edit an existing SSL tunnel, navigate to the SSL tunnels screen (**Management Console → Resources → SSL Tunnel**). A list of existing SSL tunnels is displayed.

Step 2 To edit an SSL tunnel select the **Edit** action the SSL tunnel to be altered.

This will then show a tabbed screen where values can be changed for all of the associated information against an SSL tunnel.



Step 3 Clicking the **Save** button will store the altered values and redisplay the SSL tunnels screen. Selecting the **Cancel** button will not alter any values and return to the SSL tunnels screen.

Removing an SSL Tunnel

Step 1 To remove an existing SSL tunnel, navigate to the SSL tunnels screen (**Management Console** > **Resource Management** > **SSL Tunnel**). A list of existing SSL tunnels is displayed.

Step 2 To remove an SSL tunnel, just click the **Remove** action against the SSL tunnel to be removed.

Step 3 Selecting **No** will cancel the action and return to the SSL tunnels screen. Selecting **Yes** will remove the SSL Tunnel and return to the main SSL tunnels screen.

Profiles

Profiles configure the general working environment for a user. The system provides two areas of control and they are the session and Barracuda SSL VPN Agent properties. This chapter covers all that is needed to use and manage profiles from creating to configuring them.

The sections covered in this chapter are:

- What is a Profile?
- Profiles Interface
- Creating a New Profile
- Editing Profile Parameters
- Editing a Profile Description
- Deleting a Profile

By the end of this chapter the reader should have a good understanding of profiles and how best to configure them to suit their own environment.

What is a Profile?

Simply a profile provides a means for an administrator or user to alter the general working environment of the system. Modification is encapsulated into two distinct areas those that affect a session and those that affect the Barracuda SSL VPN Agent.

The Barracuda SSL VPN Agent is an applet that tunnels data from insecure applications. The Agent intercepts the data and encrypts transmission. The SSL VPN Agent is mainly used by resources as SSL tunnels and Web Forwards.

The session parameters affect how the active session behaves and includes such things as session inactivity timeout which defines how long a user can sit idle before being automatically logged out.

Profiles can be accessed and configured by both the administrator and the user, however only the user can configure the system default profile. Users themselves - if given the permission to do so - can create and manage their own profiles.

Profiles are a great way for users to configure an environment based upon where they are accessing the system from. For example a user might configure a ‘home’ profile which is configured for use when working from home. Another might be to create a profile called ‘On-site’ which could be used for when the user is on a customer site.

Profiles Interface

The main profiles page lists the currently configured profiles. This page is located under **Management Console** > **Resources** > **Profiles**.

The main page details which policy a profile is associated with.

If a user has been given the permission to maintain profiles only those profiles associated with a user's policy are visible from the user console under **User Console** > **Resources** > **My Profiles**.

Action Icons

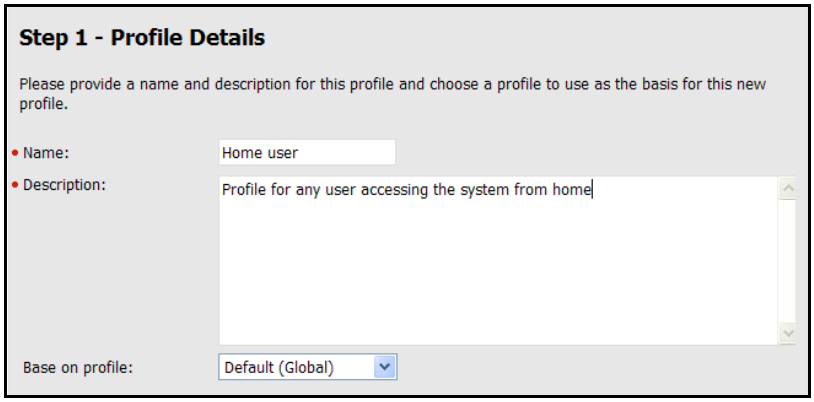
The action icons against each profile performs functions on the associated profile, their respective objective are detailed below:

	Delete profile
	Edit profile name and description details
	View or edit profile parameters (More…)

Creating a new Profile

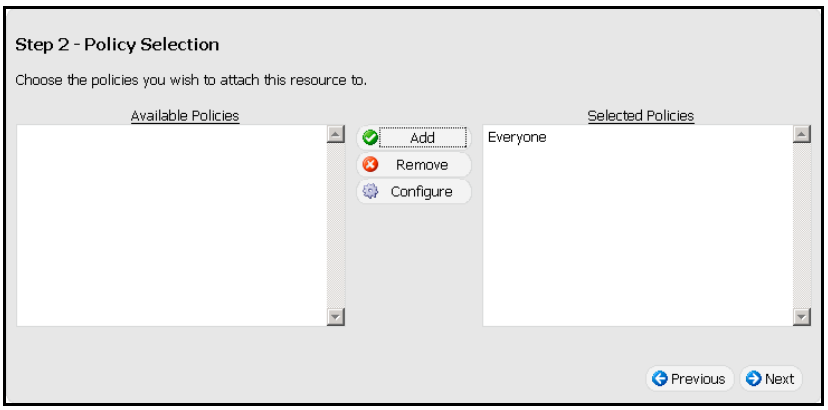
Step 1 From the main profiles page select the Create Profile action in the Action pane in the top right of the page.

Step 2 The first step in the wizard is the naming of the resource. Provide an appropriate name and description.

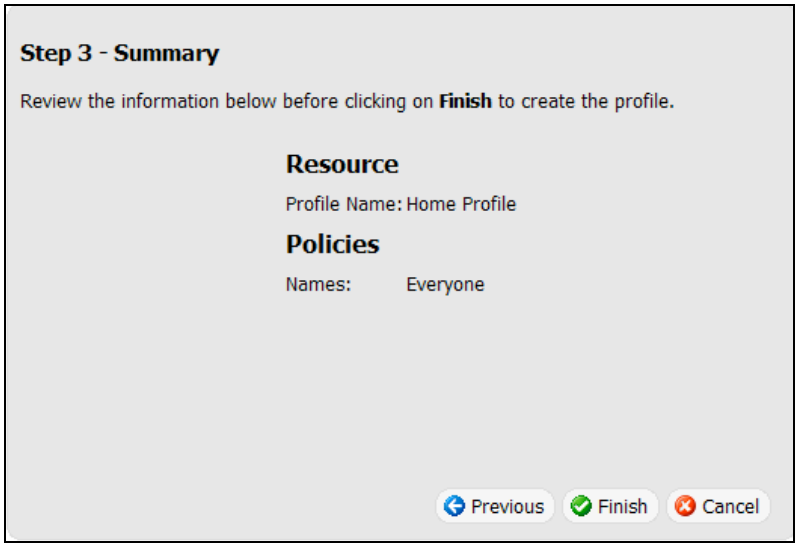

Step 1 - Profile Details
Please provide a name and description for this profile and choose a profile to use as the basis for this new profile.
• Name:
Home user
• Description:
Profile for any user accessing the system from home
Base on profile:
Default (Global)

The profile itself when created has to be based on an existing profile. All the current parameters set within this base profile are copied into the new profile. The **Base on profile** parameter should be used to select an appropriate profile to use.

Step 3 The next step is associating this profile to a policy. Select the appropriate policy.



Step 4 In the final step the wizard presents a summary of the profile.



Pressing the **Finish** button will end the wizard and create the profile.

As you will have noticed the configuration of the profile has not be done. The profile takes on the properties of the base profile. To configure this profile further the edit profile parameters action must be selected. This is detailed next.

Editing Profile Parameters

From the profiles page select the **Configure** action listed under the **More…** button against the required profile. The Edit profile page will be shown.

From here the Session and Agent properties can be altered. Selecting the appropriate icon will take the user to the edit page for that area.

Each area is detailed below.

Editing Session Details

Replacement Variables
The `${}` indicates that replacement variables can be included in the resource definition. Click this icon will load the available variables that can be used. The `session` variables are values taken from the current session. The `args` variables are values taken from user-defined attributes.

Barracuda SSL VPN Agent Configuration

- **Keep-Alive interval:** Because the Agent does not have a permanent connection to the Barracuda SSL VPN as HTTP is stateless, a heartbeat is required to inform the Barracuda SSL VPN that it is alive. If the appliance fails to receive this heartbeat then all open connections are closed.
- **Shutdown interval:** When the SSL VPN Agent is being shut down either by logging off or clicking the shutdown button a message is sent to the Agent to shutdown. If the appliance does not receive a de-registration request from the Agent within this configured interval then the appliance takes it upon itself to clean up any unnecessary connections tunnels, objects etc.
- **Registration sync timeout:** When the Agent is launched, the Agent applet downloads and tries to start the Agent. The applet then waits for the Agent to connect to the appliance and send registration request. If this is not received within this allotted time then the applet is informed and an error is raised.

No Requirement to Adjust Parameters
The heartbeat, registration and shutdown intervals shouldn't be altered unless you are working with a slow network or old hardware.

- **Start automatically on logon:** Start the Agent automatically whenever a user logs in.
- **Browser command:** Command to launch browser, leave blank for automatic.
- **Web forward inactivity timeout:** If a Web forward has been inactive for the given duration close the connection.
- **Debug level:** Set debug level. Trace gives most output, Fatal gives the least.
- **Clear cache directory on exit:** Enabling removes the Agent from the client's computer on shutdown. Disabling leaves the Agent files will be left inside a hidden directory enabling a faster start up time on next use.
- **Display information popups:** Enabling this shows messages when the Agent is performing an actions in a popup. Disabling this removes these popups and lets the Agent to operate silently.
- **Cache directory:** The location for storing downloaded applications and other resources. This directory is maintained within the users' home directory.
- **Remote tunnels require confirmation:** Enabling will force the user to accept any remote tunnel connections. Disabling will automatically create connections.
- **No session timeout if active:** This prevents the user session from timing out if the Agent is running regardless of whether the Agent has any open tunnels.
- **Localhost address:** The address to use when the appliance needs to connect to the loopback address on the client. For example, this may be set to 127.0.0.2 as a work-around for connection problems when using the RDP extension on Windows XP SP1.

SSL VPN Agent Proxy Configuration

- **Type:** Type of proxy server, this can also be configured to use whatever proxy the browser is using.
- **Hostname:** The hostname of the proxy server
- **Port:** Port number of proxy server
- **Username:** If proxy server requires authentication this will be the username provided. Leaving this blank will force authentication when the Agent connects to the proxy.
- **Password:** Associated with the above username
- **Domain:** Authenticating domain if proxy server uses Windows authentication.
- **Preferred authentication:** If authentication is used the preferred authentication method can be configured.

User Interface

- **Enable tool tips:** This enables tool tips to be shown where necessary
- **Special effects:** Enable or disable special window effects.
- **Default user console resource view:** The default view type to use when listing resources in the user console
- **Date format:** In which format should dates be used in the system

Web server

- **Session inactivity timeout:** Number of minutes a user may sit idle before the system logs the user out automatically
- **Compression:** Data received will be compressed. This has an effect on processor power but delivered data quickly.

Browser Launch

- **Reconnect if dropped:** Reconnect the browser client if the network connection is dropped. The client will attempt to connect until either an authentication failure or the user selects the exit option from the system tray icon menu. This has the effect of attempting reconnection until the browser session times out, when the session times out and authentication failure is returned. If this option is unchecked the client will remain active until the connection is dropped, the session times out or the user logs off.
- **Reconnect Interval (seconds)**: The number of seconds to wait after a disconnect before the browser client tries to reconnect the network extension. Default value is 10 seconds with a minimum value of 5 seconds and maximum value of 3600 seconds.

Editing a Profile Description

From the profiles page select the **Edit Profile Description** action against the required resource and the Edit profile page will be shown. From this page the name and description and to which policy the profile is assigned can be altered.

Deleting a Profile

The **Delete** action removes a profile permanently from the system. Selecting the Delete action against a profile will result in a warning message informing that the profile is about to be deleted.

Selecting **Yes** will result in the removal of the resource from the system. If this profile is associated with any policies this link will also be removed along with all other associated links.

System Functions

This chapter encapsulates features that affect the Barracuda SSL VPN as a whole from functions such as shutting down the server to viewing the status of the system.

Auditing

This powerful reporting tool allows for the real-time capture and analysis of user and system events. This ranges from items such as starting and stopping the system through to specific user events such as creating a favorite.

This section details how to:

- Auditing Interface
- Creating a New Report
- Running One-Off Reports

Auditing Interface

The main auditing page lists the currently stored reports. This page is located under **Management Console** > **System** > **Auditing**.

The main page details which languages have been installed and which of these is currently activated.

Action Icons

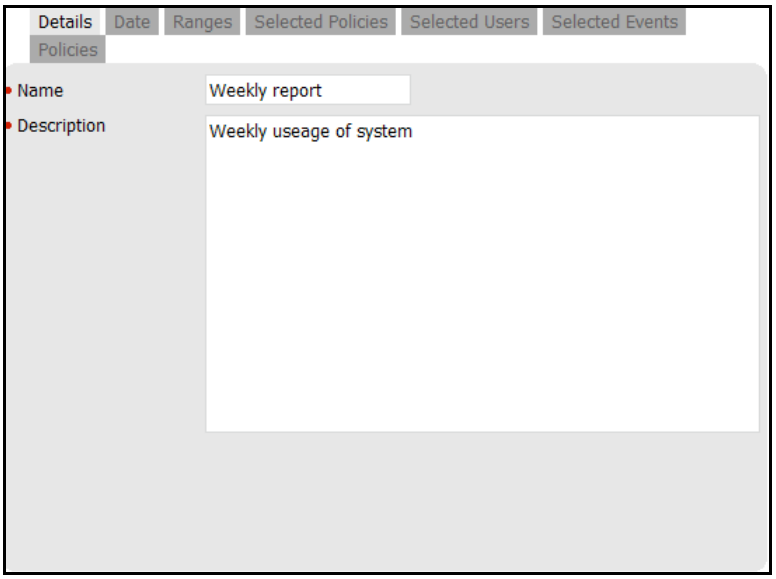
The action icons against each language performs functions on the associated language, their respective objective are detailed below:

	Delete inactivated language
	Edit a inactivated language
	Execute report
	Copy Report (More…)

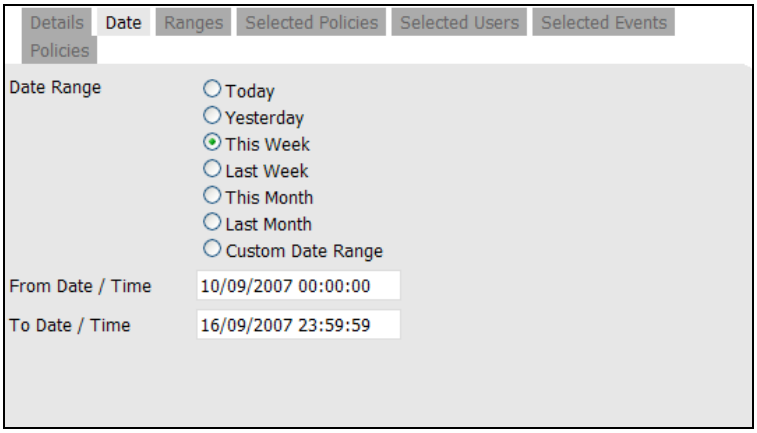
Creating a New Report

Step 1 In the main page select the **Create Audit Report** action from action menu

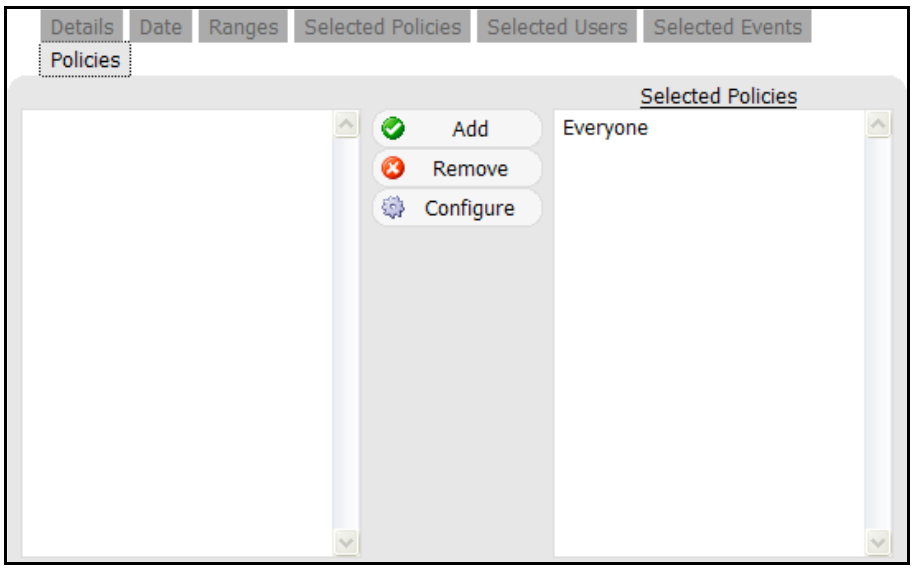
Step 2 This presents the report creation page.



All tabs contain specific information to the report, each can be configured. For example, dates can be defined in the Date tab. The report below has been configured to report on the week's auditing results.



Those who can run this report can also be defined through normal policies by selecting the policy tab.



Step 3 Once saved this report should be visible from the main page

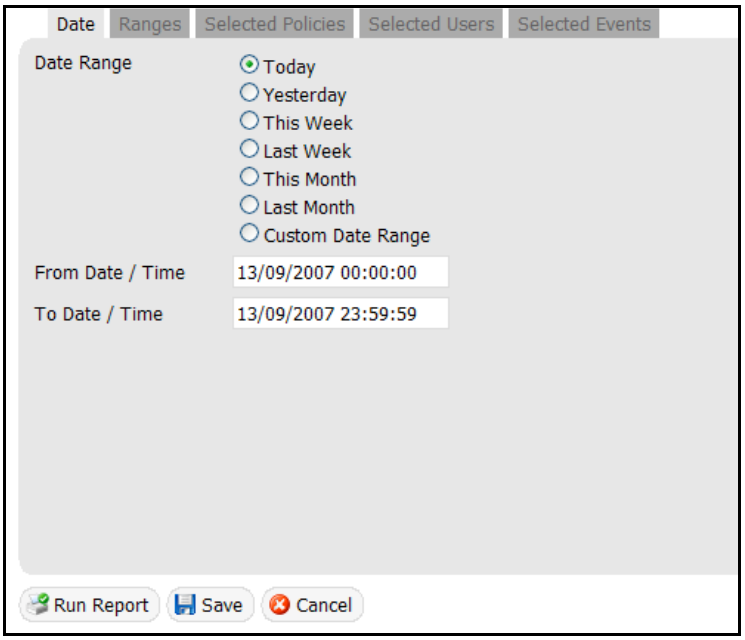
These reports can be executed over and over again by pressing the execute icon against the appropriate report. Predefined dates such as 'Last Week and 'Last Month' are run relative to the current date.

Running One-Off Reports

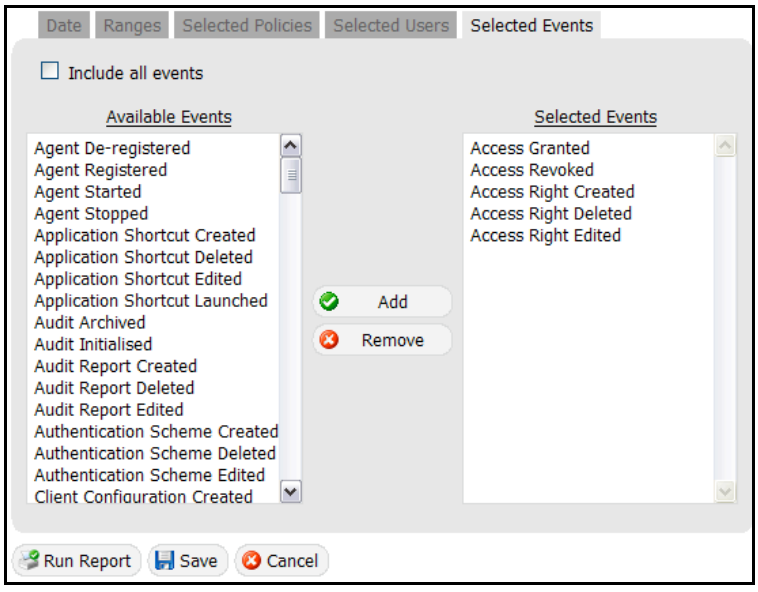
Not all reports need to be created beforehand before they can be executed. The auditing feature allows reports to created on the fly and run immediately.

Step 1 Select the 'Run Audit Report' action from the action menu.

Step 2 From here items for the report can be configured such as date ranges.

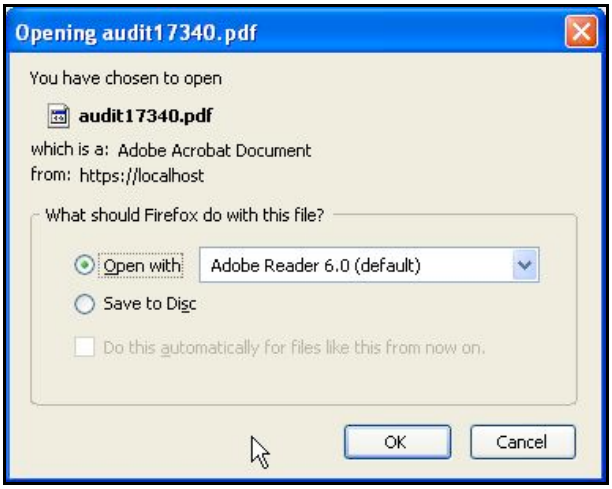


Also items like the events you wish to record.



Step 3 Once configured simply press the **Run Report** button.

This will generate the report and allow it to be downloaded. When the file download dialog appears simply save or open the file.



The report should visible once opened as below.

Appendix A

Regular Expressions

The Barracuda SSL VPN allows you to use regular expressions in many of its features. Regular Expressions allow you to flexibly describe text so that a wide range of possibilities can be matched.

When using regular expressions:

- Be careful when using special characters such as |, *, '.' in your text. For more information, refer to *Using Special Characters in Expressions* on the next page.
- All matches are **not** case sensitive.

Table A.1 describes the most common regular expressions supported by the Barracuda SSL VPN.

Table A.1: Common Regular Expressions

Expression	Matches...
Operators	
*	Zero or more occurrences of the character immediately preceding
+	One or more occurrences of the character immediately preceding
?	Zero or one occurrence of the character immediately preceding
|	Either of the characters on each side of the pipe
( )	Characters between the parenthesis as a group
Character Classes	
.	Any character except new line
[ac]	Letter 'a' or letter 'c'
[^ac]	Anything but letter 'a' or letter 'c'
[a-z]	Letters 'a' through 'z'
[a-zA-Z.]	Letters 'a' through 'z' or 'A' through 'Z' or a dot
[a-z\-]	Letters 'a' through 'z' or a dash
\d	Digit, shortcut for **[0-9]**
[^\d]	Non-digit
\a	Digit, shortcut for **[0-9]**
\w	Part of word: shortcut for **[A-Za-z0-9_]**
[^\w]	Non-word character

Using Special Characters in Expressions

The following characters have a special meaning in regular expressions and should be escaped (prepended by the backslash character \ ) when you want them interpreted literally:

Examples

Table A.3 provides some examples to help you understand how regular expressions can be used.

\s Space character: shortcut for **[\n\r\t]**
[^\s] Non-space character

Miscellaneous
^ Beginning of line
$ End of line
\b Word boundary
\t Tab character

Table A.2: Special Characters

. $
[(
])
\ |
* ^
? @

Table A.3: Regular Expressions

Example Matches...
viagra viagra, VIAGRA or vIaGRa
d+ One or more digits: 0, 42, 007
(badlgood) letters 'bad' or matches the letters 'good'
^free letters 'free' at the beginning of a line
v[i1]agra viagra or v1agra
v(ial1a)gra viagra or v1agra
v\lagra vlagra
v(il1l\l)?agra vagra, viagra, v1agra or vlagra

Table A.1: Common Regular Expressions

Expression Matches...
139
FREE *FREE*
FREE V.*GRA *FREE* VIAGRA, *FREE* VEHICLEGRA, etc

Appendix B

Limited Warranty and License

Limited Warranty

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive.

IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS PRODUCTS AND THE SOFTWARE IS PROVIDED "AS IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR-FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.

2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.

3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.

4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE

BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTIBILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.
BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B)

YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the

extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License. License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively "Barracuda Networks"), grants to the end-user ("Customer") a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the "Energize Update Software").

In addition, the foregoing license shall also be subject to the following limitations, as applicable: Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or Web Site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or Web Site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:
i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;
ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, "Energize Update Software" shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING

ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications,

capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and Agents at Customers expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.
Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.
Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph "(c)" of the "Commercial Computer Software - Restricted Rights" clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the "Technical Data-Commercial Items" clause at DFARS 252.227-7015 (Nov 1995) shall also apply.
No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Appendix C

Compliance

Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user in encouraged to try one or more of the following measures:
    - Reorient or relocate the receiving antenna.
    - Increase the separation between the equipment and the receiver.
    - Plug the equipment into an outlet on a circuit different from that of the receiver.
    - Consult the dealer or an experienced radio/television technician for help.

Notice for Canada

This apparatus compiles with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.

Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).